Understanding the West African cyber crime process

Andrews Atta-Asamoah

Introduction

Since the late 1980s, and particularly during the last decade, few mail addresses across the world have been spared the onslaught of unsolicited mail from the West Coast of Africa. In the early days many received such letters by post, later by fax and telex, and in recent times by e-mail. The content of the letters range from business proposals, inheritance reclamation, job offers, announcement of lottery wins, marriage proposals, immigration offers, admission to overseas academic institutions to money transfers and property sales, among others.

This form of crime originated in Nigeria and therefore became known as the ‘Nigerian letter’, but the phenomenon has in recent times assumed remarkable criminal dimensions through which thousands of young people operating from cybercafés in West Africa

Keywords Cyber crime, West Africa, profiling, scouting, harvesting, Internet fraud
siphon millions of dollars from victims across the world each year. In 2008, for instance, about 275,284 complaints with a total loss of US$265 million were received in the United States alone, with victims on average losing about US$931. In addition, the crime rate is estimated to have increased by about 33.1 per cent from the previous year.¹

In a region suffering from serious poverty, with rising youth unemployment rates and endemic corruption, the flamboyant display of wealth by cyber criminals has become a lure to poor and unemployed youth desperate to share in the wealth. As a result, recent trends point to the increasing involvement of young economic and social desperadoes from many countries other than Nigeria. The ‘Nigerian letter’ or ‘419’,² as the crime is known in Nigeria, has become so popular among semi-literate young people that it has seen a rapid regionalisation into a ‘West African letter’. The phenomenon is known by local names such as ‘Sakawa’ or ‘Yahoo-yahoo’ in Ghana³ and ‘Faymania’ in Cameroon.⁴ Apart from regionalisation, the crime has also evolved from the posting of unsolicited letters into a more sophisticated Internet-based criminal activity supported by document falsification, identity theft and money laundering. Further, from a crime perpetrated by disparate individuals in isolated cybercafés, it has metamorphosed into one operated by loosely organised networks who are active across several state boundaries and nationalities.

The association of the crime with West Africa has led to the area acquiring a negative label and being stigmatised internationally as the hub of Internet-based crime, and particularly advance-fee fraud (AFF). The stigmatisation of the region is such that legitimate business propositions originating from West African countries are regarded with suspicion in many international business circles. It has had the further consequence that some of the countries in the region have been blacklisted from online business transactions and payments – a situation which has had a detrimental effect on e-commerce, investor confidence and socio-economic development as a whole.⁵

In recent times, the realisation of the damaging effects of this type of crime on the region has sparked debates in many theatres of national security, commerce and development. In response, some West African countries have started to implement initiatives aimed at curbing the crime, but there is a limited understanding of the scamming process and the modus operandi of the scammers. Accordingly, scamming is continuing to flourish and the number of reported victims continues to rise across the world. It is therefore important to analyse the scamming process since an understanding is essential for formulating appropriate response initiatives.

Analysis of a typical cyber crime lifecycle

Many types of cyber crime are perpetrated in West Africa, including advance-fee fraud and black money, contract, credit card, crude oil, immigration/employment/education,
inheritance, Internet dating, lottery, property sale, reshipment, spiritual/religious and transfer of funds scams.

On the basis of their evolution and modus operandi, these crimes can generally be categorised into two principal generations. First-generation cyber crimes generally depend on a target’s willingness to accept an idea proposed by the scammer, thus making a victim’s ‘will’ an essential part of the success of the scam. For this reason many first-
generation scammers claim they are involved in a ‘trade of greed’ and that people who attempt to reap where they have not sown end up as victims. To this category of scammers, the Internet is a marketplace for selling and buying greed. These types of scams, which do not require an exceptional knowledge of computers and the Internet, include advance-fee fraud and black money, contract, credit card, crude oil, gold, inheritance, lottery, resale and transfer of funds scams.

Whereas first-generation cyber crimes focus principally on assuming a genuine and authentic tone in order to convince targets, a more complex form of cyber crime has emerged in which cyber criminals focus primarily on assuming the identity of the target. These second-generation types of crimes make extensive use of information technology skills and involve less time for an operation compared to first-generation crimes. It is a purely on-line operation which makes extensive use of phishing, hacking, website cloning and identity theft. Rather than send an e-mail to a target from the scammer’s inbox, as in the case of first-generation crimes, second-generation scammers hack and use the identity of another person (the first target) for the operation. This type of scam therefore involves two victims. By using the identity of a first victim, second-generation scammers usurp and exploit relationships that have been built by their first victim over years to exploit the second.

Though a typical scam process is principally a continuum of activities, a typical scanning process of the two generations can generally be broken down into the three stages depicted in figure 1.

**Stage I Scouting and harvesting**

This first stage of the scam process involves searching for and extracting e-mail addresses and making contact with the targets. West African scammers use various methods to harvest e-mail addresses. Some of them are:

- **Circulation of hoax mails:** Hoax messages are forwarded requesting the reader to forward the message to as many people as possible and to copy the forwarded mail to a given e-mail address. Sometimes the reader is assured that by forwarding the mails their chances of winning a particular price increase. The scammer obtains access to the e-mail addresses of all the people the mail has been forwarded to.

- **Domain contact points:** A domain can usually have up to three contact points. These are the administration, billing and technical contact points. Whichever contacts a domain has, it includes the address of the contact person. Scammers then harvest e-mail addresses from the contact points registry.

- **Forms filled in by users (on-line and on paper):** Sometimes Internet users are requested to fill in online forms, which end up becoming the user’s profile with the company
involved. Some companies make such information available on their sites as the profile of subscribers, which easily falls prey to spammers, some of whom are scammers. In some cases, the companies involved sell such information to spammers, which may include scammers. Similarly, some companies compile lists of e-mail addresses of participants of events, conventions and sell such e-mail addresses. Generally, however, the average West African scammer harvests addresses from free sources where they are not required to part with money, for example professional directories and conference proceedings.

- **Guessing e-mail addresses:** Most e-mail addresses are based on people's names. Usually the address takes the form of the first letter of the first name and the surname (for example in the case of someone named Alpha Beta, a.beta@domain) or the first and second names combined (alpha.beta@domain). This pattern makes it easy for spammers to guess e-mail addresses. By this harvesting method, a scammer guesses an e-mail address, sends a test mail or actual mail and waits for either an error message or a confirmation.

- **Hacking into sites:** Scammers may also hack into sites that supply free e-mail addresses. This method is uncommon, however, since it requires advanced computer skills.

- **Online chat rooms:** This is a major source of e-mail addresses for spammers and scammers because some chat rooms easily supply user's e-mail addresses upon request and also because it is usually one of the first public activities for new Internet users. Many scammers therefore harvest e-mail addresses from chat rooms knowing that they are valid and active addresses.

- **Profiles and e-mail addresses posted on web pages:** Some scammers make use of software capable of scanning web pages in search of e-mail addresses.

- **Subscriptions to on-line mailing lists:** In search of updates on particular topics, products or events, Internet users sometimes provide their e-mail addresses to websites. In some case such websites are clones and the subscriber is subsequently targeted.

- **AOL profiles:** AOL is generally popular among new Internet users with little or no knowledge about the modus operandi of scammers.

- **UseNet facilities:** With the aid of software, scammers regularly scan UseNets for addresses. Some of such programmes are capable of recognising and extracting e-mails from articles, especially sections containing the ‘@’ character.

- **Web browsers:** This involves the use of websites capable of extracting a surfer's e-mail address from the browser.
White and yellow pages on the Internet: Certain websites serve as people finders. Such pages contain e-mail addresses from various sources including USENet. Scammers are able to harvest names and addresses from such pages.

With the increasing advancement in Internet usage and technology across the world, e-mail harvesting has become increasingly easy. The most common approach to harvesting e-mail addresses is through the use of e-mail harvesting tools, the most popular of which is e-mail extractor software. This enables scammers to harvest thousands of e-mails from any of the above sources in a matter of hours.

After harvesting, the scammer makes the first contact with the target by e-mail and waits for a response. Typically many recipients treat unsolicited e-mails as spam and do not respond, although they do not necessarily delete the e-mail from their inboxes. Scammers on average have a less than 2 per cent response rate to the mail they send out.

If a target does respond favourably, scammers proceed to stage II of the scam lifecycle. In cases where scammers are part of a network, the scouting and harvesting process is the responsibility of apprentices and protégés. After a fruitful contact is made by a protégé, the target is passed on to more experienced scammers who assume the identity used by the protégé in the initial contact and communication.

Where hacking and phishing are involved, as is the case in second-generation scamming, this stage involves scouting for a particular e-mail to hack or website to clone in order to assume the identity of the victim during the other stages.

Stage II Relationship building and profiling

In the second stage the scammer will attempt to build a relationship with the target, ranging from friendship and business to social relationships. As the relationship becomes close and deepens through frequent communication, the scammer profiles the target. Scammers usually carry out target profiling by requesting or gathering information about the target's nationality, profession and age, in the process acquiring a photo, a copy of the information page of a passport/identification document, and sometimes bank account details. This information enables the scammer to determine the 'juiciness' of the target. If targets are profiled as 'dry', they are discarded from the scamming radar. On the other hand, communication is maintained and strengthened in the case of 'juicy' targets and the scammer will proceed to stage III.

Stage II requires great tact and care to avoid the victim from becoming suspicious and therefore cybercrime networks generally use more experienced members for this stage of the scam. This stage could last as long as it takes the scammers to build up a strong relationship from which they are able to profile the target (see 'target profiling (1)' in figure 1).
If hackers and website cloners are involved, the relationships built by the first victim are usurped for the exploitation of the second victim.

**Stage III Operational stage**

This is typically the stage during which the scammer proposes an idea involving the transfer of money or goods. Experienced scammers proceed cautiously at this stage since any wrong or suspicious move could strain the relationship and allow the target to escape. As indicated in figure 1, the scammer will propose a new idea if the target is not interested in the first proposal. However, if the target does take the bait, the scammer quickly but cautiously proceeds to ask for the transfer of funds or goods. If the target does transfer the requested funds, the scammer will return to the profiling process (see ‘target profiling (2)’ in figure 1).

At this stage, the scammer seeks to primarily establish whether the victim has the capacity and willingness to pay more. If not, the victim is discarded and the relationship and communication end abruptly. If the likelihood is good, however, the scammer devises a new reason or scheme for obtaining an additional payment or transfer of funds, and so on.

The cycle of money requests and transfers continues until the victim is either unable to transfer additional funds or becomes suspicious. If this happens, the scam cycle is broken. The operational stage can thus last as long as the victim is ready to transfer funds or has not become aware of the scam. In extreme cases a scammer or a network sells the contact details of the victim to another scammer who will start the entire scam process all over again.

**Conclusion and recommendations**

A review of the scamming process provides important insights and entry points for curbing this type of crime. In the first place, it is clear that many Internet users expose themselves to scam e-mails by responding to calls to complete forms, by circulating e-mails, or by subscribing to e-mail alerts from untrustworthy websites, purely as a result of ignorance. Second, with increasing practice, the nature and methods of scamming are rapidly evolving in sophistication. The more sophisticated scammers become, the more difficult it is to curb their activities.

It is important that actions aimed at curbing the crime takes into account five main strands of activity:

**Education**

Internet users, particularly in developed countries, should be educated about the modus operandi of scammers and the dangers associated with visiting sites with malicious
content. This will help reduce the susceptibility of Internet users to harvesting and the likelihood of falling prey to scammers. For instance, they should be taught or learn how to identify scam e-mails and how to avoid being profiled by scammers. Online businesses in particular need to monitor their websites regularly to prevent cloning.

**Web-based snare programmes**

One important deduction from the scamming process is that with an organised technology-based approach, scammers can be trapped. This could be achieved by initiating web-based snare programmes using undercover investigators who will pose as victims. Through undercover operations, ringleaders in the scamming cycles can be busted thereby reducing their activity.

**International cooperation**

However, such web-based snare programmes call for strengthened collaboration and cooperation among security agencies in countries of both the victims and the perpetrators. Given the trans-border nature of the crime, it is also important that Interpol considers giving greater attention to it. International cooperation and the involvement of Interpol will help to bridge the distance between scammers, victims and law enforcers in fighting the crime.

Efforts should also be made to bring on board private enterprises, which are usually key in any scam process. These include money transfer services, banks and Internet service providers and Internet protocol operators.

**Institution of appropriate legal framework**

To provide the framework for collective action, West African countries need to harmonise cyber-related laws with which the crime can be prosecuted in the individual countries and regionally. The responses of countries in the region should be as even as possible in order to curb the redistribution of the menace through the relocation of criminals across borders.

In addition, there is the need for countries in the region to institutionalise the response, as Nigeria has done. This will help prevent ad hoc responses which have the capacity of pushing cyber crime networks underground and making the crime difficult to stem in the long term. As part of institutionalisation, specialised law enforcement units equipped and trained to combat the crime should be formed. It is unthinkable that ill-equipped state institutions will succeed in curbing a modern and technology-based crime such as cyber crime.

Globalisation has propelled cyber space to the fore as one of the frontiers of a state's territory and a turf where the state needs to assert its territorial integrity. So far, the
cyber crime menace has been demonstrating how governless this new frontier on the African continent has become. The earlier efforts are made to contain the menace and assert control in the virtual frontier, the better for the continent and the world at large.

**Notes**

2 The name ‘419’ was coined from section 419 of the Nigerian Criminal Code, which is the principal legal instrument that criminalises the phenomenon in Nigeria.