**The Observe Phase**

The methods that we adopted in the Observe Phase are:

* Interviews
* Unobtrusive Measures

Our findings were documented using the What? How? Why? approach as seen below:

**Interview**

**Interviewee**: Mr. Benjamin Ude (fictional name)

**Sex:** Male

**Age bracket**: Early 30s

**Ethnicity**: Igbo

**Nationality**: Nigerian

**Skill:** former perpetrator of love scam on the Internet

**Years of operation:** 2 years

Currently an entrepreneur

1. **What are people doing?**

Of course, youths are engaging in cybercrime but can you really blame them? They are only trying to break out of the slavery that the government has imposed on its citizens because nothing is really working in this country.

You will see government officials that literally do nothing cashing out and living large while hardworking citizens that labor day and night won’t even be able to afford three square meals.

What do you expect then? They will have to find a way to make ends meet na by going into activities that will give them fast cash so that they can also live large. Activities like raiding people’s bank accounts online, stealing people’s identity and sometimes even impersonating them to scam unsuspecting victims, doing things like love scam online to cash out (this one is even like the most common one now; they will register on dating sites, meet people online, pretend to start a relationship with them and then as time goes on, they will start getting financial favors and stuff like that from them), setting up online trading platform where people invest and get scammed.

This is just to mention a few.

1. **How are they doing it?**

Well, how the youths engage in cybercrime basically depends on the kind of crime they are committing.

Just like l explained earlier about the Love Scam; they engage unsuspecting victims on dating sites and get them to do financial favors for them or even go as far as deceiving them to invest in non-existent business opportunities all in the name of building relationship and planning future with them.

The one about identity theft and impersonation is basically the perpetrators posing like someone else and getting victims to part with cash. You know the popular one na, where someone will hack your WhatsApp and send messages to your family or loved ones telling them that you are in dire need of money for one reason or the other.

Your family members or loved ones will send their money thinking the request is coming from you and so on.

They can even steal login credentials for people that work in financial institutions and use that to siphon money from the system.

You also know of another common one where once your phone is stolen, they will use that to wipe all the funds in your account by logging into your online Application or even using the USSD code.

1. **Why are they doing it?**

The country’s economy is nothing to write home about. The government is not treating the youths right and even some level headed youths that are striving to become entrepreneurs are being frustrated government policies that cripple their businesses. No government jobs, no incentives or fair policies that will favor SMEs, no grants or loans for startups; even banks self are not giving loans anymore and if you manage to get loan, the interest alone will swallow any profit you ever make.

So, naturally the youths wouldn’t want to labor in vain and so they will rather engage in cybercrime to cash out quick.

Another major reason why the youths engage in cybercrime is that the government does not listen to the people! They don’t understand the people’s plight. But how can they when they don’t even listen to them.

It’s one thing to keep doing things you think might help people and it’s an entirely different thing to do what the people tells you will help them. The two things will produce different results.

So, the government need to first listen to the people and get to understand the problem they are facing that made them to go into cybercrime and also learn from them, what they can do to make them stop.

The government of Nigeria is just very selfish. They only look out for themselves and their loved ones; that’s why you see them sending their own people outside the country because they know that they have not created a conducive economy for anyone to succeed and thrive.

So, what do you expect, the youths who are left behind and do not have anyone to sponsor their Japa (leave the country) will definitely have to start looking for ways to make end meet and so they turn to a get-rich-quick approach that they can easily get away with even when they catch them.

A good government is not selfish; it will look out for all its citizens and by so doing, the citizens will learn to also look out for others and before you know it, they will build a culture of look out for one another and it will keep spreading and eventually become their way of life.

Another thing is that the government has built a system where almost everyone depends on them to survive. And a government that makes people to depend on it will keep running them as slaves; and so, the people will become frustrated when the government fails to pay them or do things for the. And in a bid to break out of that slavery, they will then turn to cybercrime to cash out quick.

The major problem of the Nigerian youth is that they are living on survival instinct.

All the systems in the coin are not working.

And you may why the youths are not going into other criminal activities. Why cybercrime? The thing is that almost every young person in Nigeria has phone and internet access is relatively affordable. So, it’s not even hard for them to go into it.

And when they are in it and they get caught, the possibility of sorting themselves out with the authorities is very high. All they need to do is to give whoever catches them enough cash and get released. Because they have the money to do that. Everyone in this country is just so corrupt!

Of course, you know that yahoo boys earn more than legit civil servants and even business owners.

1. **Other Comments**

The truth is that corruption has eaten so deep into the fabrics of this country that any effort to stop cybercrime might not work until that issue of corruption is severely dealt with.

The reason why corruption still thrives is because no one is being held accountable for their actions and we are all being controlled by money.

A country where someone can just come out and claim that snake swallowed money and insects ate receipts and still go scot free. What do you expect? So, the young boys and girls will also feel like they can do anything and get away with it; so long as they have money to pay.

The government need to place trustworthy people in positions that matter and ensure that everyone is held accountable for their actions.

I know you said something about creating a hub where people can make complaints but it is not about reporting cases.

The real problem is, when complaints are made, what happens to the culprits? That is the real problem!

People report cybercrime on daily basis but nothing happens to the perpetrators and that is why people are discouraged to make reports.

And the reason why the culprits go free is because they have money to sort themselves out when they are caught and no one will even follow up to confirm if they are prosecuted or not.

The day there is order and law enforcement in this country is the day that cybercrime will reduce drastically. There is law against cybercrime but we don’t practice it because there is no order.

Broadcaster prosecution of cyber criminals will help with creating order. Because at least, everyone will see that the cyber criminals are being punished (it will encourage them to bring complaints forward) and other youths who intend to venture into the field of cybercrime will think twice because they know that when they are caught, they will be publicly prosecuted.

In conclusion, l can sit here and proffer solutions on what needs to be done but the truth is that without serious government intervention, much impact will not be made.

The key to drastically reduce youths’ engagement in cybercrime lies with the Nigerian government.

**Unobtrusive Measures**

1. **What are people doing?**

Nigerian youths engage in cybercrime activities like raiding bank accounts, identity theft, impersonation, stealing of corporate information, love scams, online trading scams, hacking, software piracy, pornography, credit card or ATM fraud, denial of service attack, virus dissemination, phishing, cyberplagiarism, cyberstalking, cyberdefamation.

1. **How are they doing it?**
2. **Free ticket/voucher scams**

This cybercrime comes as gift cards to popular stores or restaurants. They are advertised in emails as ads on websites or shared in some social media handles. Once someone falls victim and clicks on the freebie’s link, he/she can be scammed and the perpetrators usually harvests secret information related to bank accounts or assets.

1. **Cryptocurrency scams**

According to Button and Cross (2017), in this type of cybercrime, victims will be invited to sign up to crypto currencies in social media or so-called investment sites, and once the person falls victim to this scam, their personal information will be retrieved and used for further hacking. In some cases, victims realize that they have been defrauded only after the website has been deactivated and suspects can no longer be contacted. According to the Federal Trade Commission (FTC) Consumer Sentinel, from October 2020 through March 31st, 2021, reports of crypto scams skyrocketed to nearly 7000 people reporting losses of more than $80million. These figures reflect a 12-fold increase in the number of reports compared to the same period a year ago and a nearly 1000% rise in reported losses (FTC 2021)

1. **Personal data fraudsters**

Personal data fraudsters usually persuade victims to send their personal data for a promo or other scams. Once retrieved, the perpetrators will clone the identity of the victim and use it for their benefits. This is usually carried out in most social media platforms (Button and Cross, 2017).

1. **Free trial products**

Social media sites are often used to lure people into signing up for free trial on products. These scams usually involve the participants signing up for a free trial of a product which is often not genuine, instructing them to provide their card payments details upfront (Tade, 2013). The victim then becomes tied into a fixed period of contract unbeknownst to them and have provided their card payment details to an unknown individual.

1. **Investment scams**

In this type of cybercrime, opportunities are advertised on social media sites for people to invest in products or businesses which are often fake or do not exist. Fraudsters advertise a too-good-to-be-true investment opportunity, sometimes using new stories and advertisements that appear to be from genuine sources (Tade, 2013). Consumers who are tempted to invest lose some or all of their money.

1. **SOS or help messages**

This scam involves social media account holders receiving messages from persons in their “friends” or “contacts” lists indicating that they are in trouble in a foreign country and need help (Ezea, 2017). This message usually request that they transfer money to an account in a foreign country. The content of the message varies but popular ones tell the story that the person has been arrested and needs money for bailing. Once someone falls victim to this scam, a huge sum of money is pulled out of their bank account (Ezea, 2017). In one specific variant, the text directs the victim to a website and offer them a small gift (like a wristwatch) for participating in a survey.

1. **Fake friend requests**

In this kind, social media account holders will receive friend requests from people that they do not know or people already in their contacts who have had their accounts hacked (Ezea, 2017). Accepting these requests causes the account of the victim and that of their friends to be hacked, and their entire personal data accessed.

1. **Why are they doing it?**
2. The three-prolonged advent of the internet, computers and mobile devices gave rise to the massive outbreak of cybercrimes.

Cybercriminals leverage the anonymity provided by the Internet to defraud unsuspecting victims.

1. Cybercrime is rampant in Nigeria because of the rapid digital business migration and dependency and easy access to internet connectivity.
2. Youths engage in cybercrime because of erosion of societal values arising from a growing negative influence of politicians who rise to wealth suddenly through appropriating state resources for their private use. The get-rich-quick syndrome is a huge influence as the youths try to make it at all costs.
3. Cybercrime appears attractive to many youths particularly because the probability of getting caught is low and the criminals have the physical and technical resources to evade capture. Basically because cybercrime is **lucrative** and **hidden.**
4. Digital revolution of e-banking has created an enabling environment that resulted to an equivalent revolution in e-banking frauds.
5. Increasing access to digital literacy, near pervasive internet availability and access to smart devices
6. Insufficient/inadequate/weak cybercrime policies and infrastructures that track cyber criminals and enforce cybercrime laws when they are caught.
7. Many youths engage in cybercrime because the challenge and fun entice them. Others engage in it out of ignorance; because they are not aware of the negative implications.