# Cybertheft in Africa: Social Engineering challenges in perspective.

**Dr. Yawo O. Kondo** * Études internationales, Université de Nebraska* Administration de l'informatique de la santé, Université de Maryland* Technologie de l'information, Université de Walden* Contact : Konyaw4310@gmail.com

I received a message from a gentleman in Africa requesting advice on cybertheft. I told him this was a broad topic, and I could only help him if he were specific. Someone has fraudulently emptied his savings account. He went to talk to the account manager, who tried to question his credibility. What happened? Was it a cybercrime? Was that possible? Does he have any protection? Many are the questions he wanted me to answer.

A new type of illegal activity emerged in Africa with a high Internet accessibility rate. This type of cybercrime is known in West Africa by different names: Yahooman, 419, Gaymans, etc... Cybercriminals pose a threat to the economy of Africa. Not only do these threats present challenges to businesses, but also, they affect the cyber resilience reputation of the countries. These crimes are different from the crime in other parts of the world. Africa's infrastructures are predominately mobile phone web traffic due to the cheaper mobile connections, which do not require additional infrastructure such as a fixed-line internet connection as with desktop computers. Therefore, cybercriminals target more mobile networks than computer infrastructures. Smartphones account for up to 74% of all web traffic in Nigeria, while personal computers account for 24%. Up to 81% of South African households in metropolitan areas only use mobile phones at home. According to data on Internet penetration in Kenya, in 2018, 95.1% of adults in the country subscribed to mobile phone services, while 42.9% had access to broadband internet.

The majority of cybercrime committed on the continent is through social engineering, phishing, and false promises, such as opportunities to buy products, provide services, invest money, or receive free product trials. This is how cybercriminals harass customers of mobile money platforms, economic operators or anybody they can scam. Cybercriminals use social media groups to conduct malicious social engineering attacks to steal confidential or personal information. These groups become a lucrative target because social network users frequently provide sensitive personal information such as mobile phone numbers or email addresses without realizing the risk of their actions. Despite the mobile network increasing crime incidents, there is also a growth in computer scam threats. Hackers seek to exploit various security holes and slack cybersecurity practices that can allow them to steal or modify digital information. As reported, Cyber Horus Group cyberattacked Ethiopia in June 2020 and hacked into various Ethiopian government websites, posting war messages in case Ethiopia goes ahead with its plans to fill the GERD dam. The hacktivist group Anonymous launched #OpAfrica in South Africa and

compromised 33,000 records, exposing the personal information of up to 1,500 government employees. Kenya's Integrated Financial Management System (IFMIS), Immigration Department, Judicial Service Commission (JSC), Petroleum Ministry, Refugees Affairs, and Kenya Meat Commission were targeted in 2019. Hackers stole or attempted to steal $61.5 million from various financial institutions in Ghana, according to a 2018 report by the Bank of Ghana. In Togo, it was reported that one of the leading banks allegedly was the victim of cybertheft last year. Nigeria recorded a loss of $649 million in 2017, while Kenya lost $210 million due to cybercrimes.

In 54 countries on the continent, according to a 2013 report, 30 do not have explicit cybercrime and personal data protection (PDP) laws. It will be challenging to fight cybercrime on its territory or against neighboring countries without legislation. Several African governments are developing legislative frameworks and policy instruments at various stages. However, most countries need more technical knowledge to monitor and protect their national interests. Togo is one of the African countries with explicit cybersecurity legislation that guarantees online privacy and personal data protection for all users. "Law No. 2019-014 of 29 October 2019 on the protection of personal data" and "Law No. 2018-026 on Cybersecurity and the fight against Cybercrime". The country's cybersecurity legislations emphasize preserving confidentiality, integrity and information availability and defining the responsibilities. These legislations on the continent need the mechanism to reinforce the laws for several reasons.

How is it possible that this gentleman did not use his card but lost his saving? From a cybersecurity perspective, it is possible through social engineering attacks such as baiting or smishing. A baiting is a social engineering attack in which scammers make false promises to users to trick them into revealing personal information or installing malware on the system. The gentleman could also receive a message with a link in the form of smishing. SMS phishing is a social engineering attack conducted specifically by SMS. In this attack, scammers try to trick the user into clicking on a link that takes them to a malicious site. Once on the site, the victim is prompted to download malicious software and content. These attacks can happen either on the customer's or financial institution's networks. However, financial institutions can use legislative frameworks and policy instruments to mitigate these attacks. It will be in the interest of all financial institutions in this to follow the Payment Card Industry Data Security Standard (PCI DSS) framework. One must ask whether the two actors (the bank and the customer) have the necessary technical knowledge to monitor and protect their networks.

The account manager only has to open a ticket with the incident report from the customer. Then someone will check the review transactions log and escalate that to the Security Operations Center team for technical review to determine if the customer has withdrawn the

money. Non-repudiation guarantees the availability of evidence that can be invoked against a third party and used to prove the traceability of electronic communications that have taken place.

There are anthropological and phenomenal explanations for African countries' inability to address the continent's cyber threat. The undermined poverty, systemic corruption, and misgovernance force a portion of young men into cybercriminals. They engineer malicious social attacks, harass, intimidate and make false promissory. It is difficult for governments to fight these crimes because the community these criminals live in becomes an accomplice. In many cases, people in the communities know the status of the unemployed cybercriminals who live big on cybertheft.

Africa must prioritize cybersecurity, create a workable legal framework to manage the threat, and consider harmonizing national legislation, standards, rules, and guidelines regarding cybersecurity challenges due to cybercrime's worldwide and cross-border nature. Internet users should maintain the RADAR when dealing with emails, links, emails, links, social media posts, and advertisements. They should check the URL before sending personal information online and avoid to click on anything suspicious and answer messages requesting sensitive information sent via email.