28 - 30 September, 2022 / Prague, Czech Republic

THE LONG ARM OF THE PRISONER: SOCIAL ENGINEERING FROM KENYAN PRISONS

Patricia Musomba & Tim Dagori

Co-Creation Hub, Kenya

patricia@ihub.co.ke
tim@ihub.co.ke

ABSTRACT

Prisons serve four main functions; retribution, incapacitation, deterrence, and rehabilitation. Retribution is achieved by depriving criminals of their freedom and incapacitation through the removal of criminals from society so that they can no longer hurt innocent people. While serving sentences, prisoners go through rehabilitation programmes to become law-abiding citizens and deter future criminal activity. However, with the advent of technology, these four functions are impeded since prisoners can gain digital freedom to perpetrate criminal activities through smuggled mobile devices.

Using social engineering, Kenyan prisoners have utilized mobile phones to defraud citizens of their hard-earned money. While this has long been the case, a recent uptick in scamming incidents has drawn the attention of the media, the government, the security community, and the general public. Over time, the scams have become more sophisticated. For example, in early 2022, a prisoner serving a life sentence at Kamiti Prison confessed to scamming a job applicant of Ksh 800,000 by impersonating the Defense Cabinet Secretary.

Through an in-depth investigation of data posted on social media and news sites, this research reports on the social engineering strategies used by convicts, such as baiting, pretexting, vishing and smishing. It also recognizes the tell-tale indicators, such as instilling anxiety, a sense of urgency, and requesting sensitive information like mobile money PINs. Finally, it presents ideas on how to minimize the expanding threat.

INTRODUCTION

According to a *Business Daily* survey in 2021, half of Kenyans using mobile money have lost money through fraud and scams [1]. In a country where mobile money has deepened financial markets and encouraged financial inclusivity, this is a staggering statistic, warranting attention from the public and private sectors. Despite mitigation efforts such as legislation, raising awareness, and incorporating fraud controls in mobile money applications, mobile money scams are still a menace. From recent reports, most of these scams emanate from prisons.

With the increased use of technology for conducting business, learning and socializing, the cybercriminal's playground has extended beyond physical borders. This has particularly benefited prisoners, who can use smuggled digital devices to perpetrate criminal activities despite being physically locked up. Most Kenyans have received a message or a call from the so-called Kamiti Boys, a term coined from frequent reports of prisoners from Kamiti Maximum Security Prison duping Kenyans [2]. While there are cases of scams from other prisons across the country, this paper will specifically use the Kamiti prison as a case study due to the availability of extensive reports and testimonials.

Reports show that prisoners make calls to random phone numbers or send scam messages to unsuspecting Kenyans hoping to find their next victim. There is a method to this madness that employs the art of deception, otherwise known as social engineering in the information security world. How do locked-up criminals convince Kenyans to part with their hard-earned money?

SOCIAL ENGINEERING TECHNIQUES

Humans are often the weakest link in the cybersecurity ecosystem, mainly because of their trusting nature and tendency to lean towards the benefit of the doubt. This is the foundation of all social engineering attacks. Social engineering is a cyber attack that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Cybercriminals use that information for various purposes including financial gain, perpetrating other attacks, or damaging reputations. In the case of Kenyan prisoners, the motivation is singular: financial gain.

Anatomy of a social engineering attack

Although social engineering attacks differ, they follow a common pattern with similar phases. There are four phases to any social engineering technique as shown in Figure 1 [3].

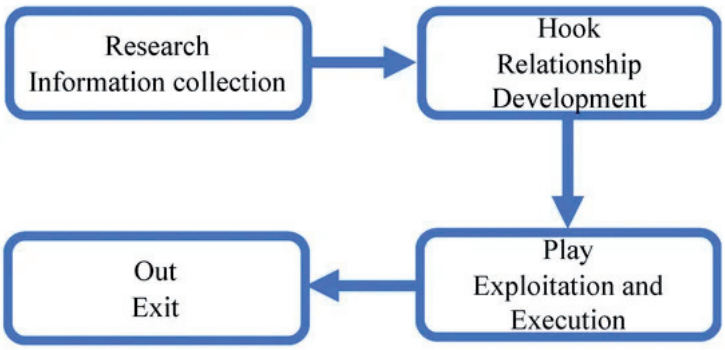

Figure 1: Social engineering phases.

An attack begins with research to gather information about a target. This information is used in the next phase, where an attacker initiates contact with the victim to develop a relationship with them. Having extensive details on the target encourages trust, making it easier to forge a relationship. Once the victim is hooked, they are more likely to be emotionally influenced, hence the attacker proceeds to exploit the relationship. In the 'play' phase, the attacker solicits favours or asks for sensitive information such as mobile money PINs. In the last phase, the attacker detaches from the victim, in most cases, leaving little to no proof.

Techniques utilized by prisoners

Due to physical limitations, physical social engineering attacks such as shoulder-surfing, dumpster diving, and tailgating are difficult. Hence, prisoners lean towards technical attacks conducted through social networks and online services websites. The techniques employed in prisoners' '*tuma kwa hii number*' (send to this number) scams include phishing (smishing, vishing), pretexting and quid pro quo.

Phishing

Phishing is a type of social engineering attack that is frequently used to steal sensitive user information such as login credentials and credit card numbers. An attacker poses as a trusted entity and tricks the victim into opening an email, instant message, or text message. Prisoners mainly rely on messages (smishing) and calls (vishing) to communicate with unsuspecting Kenyans. Both techniques have similar tell-tale signs such as conveying a sense of urgency, too-good-to-be-true scenarios, and unusual requests like money.

Prisoners use feature phones as their weapon of choice mainly because they are relatively easy to smuggle in and have specific capabilities to perform the attacks. For instance, the *Itel 5170* comes enabled with a voice-altering feature, popularly known as the 'magic voice', allowing an attacker to switch their voice to a man's, woman's, or a child's. The inbuilt voices are mostly foreign (American or European), allowing prisoners to run scams based on a foreigner pretext.

Pretexting

Pretexting attacks involve the creation of fictitious and convincing scenarios to steal a victim's personal information. The attack is carried out through phone calls, emails, or messages and relies on pretexts that encourage the victim to believe and trust the attacker. The pretexts below have delivered huge pay-days for prisoners:

- **Radio station cash prizes**. An attacker contacts a victim to inform them that they have won a prize with a local radio station. The attacker then tells them to send money to redeem the cash prize or to facilitate the transfer of the prize. This pretext mostly targets rural inhabitants whose knowledge of digital safety may be lacking. In one news report by *Citizen TV*, a prisoner admitted that they use this pretext on house girls and gatemen.
- **The stranded foreigner**. The attacker fakes an accent, or utilizes the magic voice feature on some feature phones to create a foreign identity. This pretext mostly targets women. The attacker will attempt to create a romantic relationship over some time while pretending to be an expatriate posted in a different town. Once the target is hooked, the attacker will arrange to meet in the target's town and even proceed to share hotel details of where he'll be staying. However, in the course of the fictitious journey, he will pretend to be stranded, for example, at a filling station, and claim to need money in order to continue. The victim will even have a conversation with an attendant to continue the ruse. Most victims will send money, and be the heroes of the day, only to be ghosted after the transaction has been completed. The pretext can also work through SMS, as shown in Figure 2.

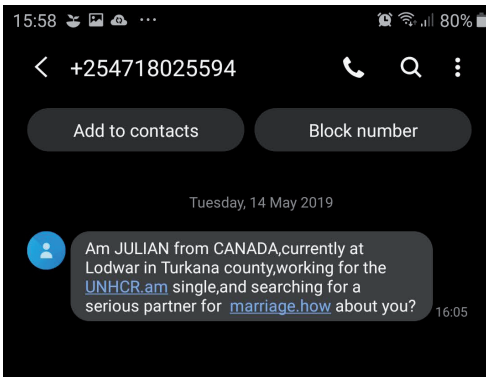

Figure 2 Smishing message screenshot.

- **Greener pastures**. The attacker in this pretext promises to make travel and employment arrangements for the victim to travel to different destinations. They request personal information to use for the itinerary. Over time, the attacker sends flight details, employment letters, and entry letters into the country of choice. Finally, the attacker asks the victim to pay a certain amount in taxes that are 'required' by the country. This is a long con pretext.

- **Current events**. Prisoners have access to information on current events, therefore, some pretexts will be based on that. For example, when the first case of Covid-19 was detected in Kenya, many institutions closed down. A popular pretext preyed on parents' anxiety over their children getting home from boarding schools. The scam message shown in Figure 3 translates to '*Hi Mom, the school was closed today morning because of Corona Virus. Please send bus fare to teacher David*.'

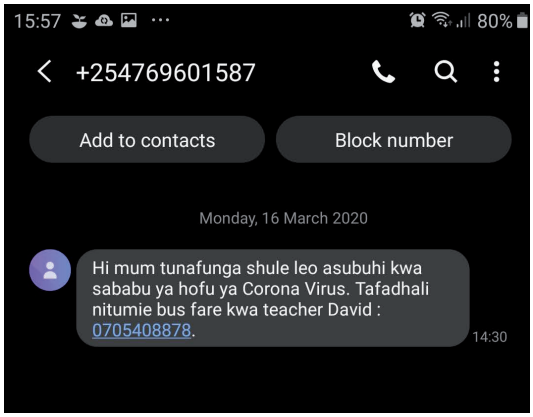

Figure 3: Smishing message based on Covid-19 pretext.

Quid pro quo

The main characteristic of a quid pro quo attack is the give-take exchange. The attacker asks the victim to divulge information or perform an action and they will be rewarded with something. For prisoners, this mainly happens with mobile money platforms. For example, the attacker sends a fabricated mobile message claiming to have sent money to the wrong phone number and requests the victim to send the money back, and receive a cut. Another example of quid pro quo is when an attacker promises to arrange employment for the victim but asks for some form of payment once the victim receives the offer letter. Such is the case of Dr Selina Vukinu Ambe.

Case study

Referencing media reports, challenging economic times contribute to the success of many scams since most scams promise money or greener pastures. A prisoner serving a life sentence at the Kamiti Maximum Security Prison conned Dr Selina Vukinu Ambe, swindling her of 800,000 Kenya Shillings [4]. The prisoner, Patrick Shikure Amere, promised Dr Ambe a position as the State House Human Resources Manager through a series of online communications and phone calls. He also confessed to impersonating the Defense Cabinet Secretary Eugene Wamalwa to carry out the scam. The con happened between 24 July and 11 September 2020, while the case was heard in February 2022.

The Computer Misuse and Cybercrimes Act of 2018 [5] criminalizes computer forgery, computer fraud, and phishing. Whilst these offences attract hefty fines and prison terms they are not enough to deter prisoners who are already incarcerated.

MITIGATION

Proactive and reactive measures need to be implemented to stem the growing number of online scams. These measures include localized security training, improved infrastructure, and improved security in prisons.

Localized security awareness

As illustrated in this paper, some scams target rural communities where security awareness is minimal. Most security awareness training is done by private companies working in the financial sector, with English and Swahili as the preferred languages. To better educate all citizens, localized content is needed. Content in the different vernacular languages can be very effective and can enhance knowledge retention. Campaigns run through radio stations and bulk text messages would reach most Kenyans, especially those in rural areas and those using feature phones.

Additionally, collaboration between the government and local community organizations, particularly those working on technology inclusion and digital literacy, can drive local security awareness efforts.

Improved infrastructure to handle cybercrime – National Forensic Lab

Cybercriminals' tactics, techniques and procedures have greatly progressed with advancements in technology. However, most governments, especially those in developing countries, have not invested in proper infrastructure to prepare, detect, and respond to various cyber threats. Following an increase in mobile money transactions and the subsequent rise of digital

economy crimes, the Government of Kenya is now directing resources to building infrastructure. For instance, during the commissioning of the National Forensic Lab [6], the president reiterated the importance of the lab in curbing the new wave of digital attacks such as SIM swapping and the Kamiti Boys' '*tuma kwa hii number'* (send to this number) scams discussed in this paper. The lab is expected to fast track the investigation of serious crimes such as fraud, robbery, terrorism and cybercrime, among others. Such infrastructure and cyber capability can enable faster incident response and investigation.

Improved security in prisons

Finally, since the menace originates from Kenyan prisons, there is a need to improve physical security in prisons. This will reduce the likelihood of prisoners smuggling mobile devices and operating a 'call centre' within the premises. Following news reports of the illegal call centre at Kamiti Maximum Security Prison, a police spokesperson made a statement to reassure Kenyans that the police and prison department were keen to implement serious security measures to dismantle the Kamiti Boys call centre [7].

CONCLUSION

Implementation of the mentioned interventions would go a long way towards curbing most cyber scams, not just those emanating from prisons. Security professionals can spearhead the conversation and offer their time to educate the masses. What may be trivial to the security professional, may be eye-opening to others.

REFERENCES

[1] Business Daily Africa. Survey finds half of mobile users lose cash to fraudsters. December 2021. https://www.businessdailyafrica.com/bd/economy/survey-finds-half-mobile-users-lose-cash-fraudsters-3654490.

[2] Monzon, L. Kenyan 'Kamiti Boys' Fraudsters are Cleaning Out Mobile Cash Wallets. IT News Africa. March 2020. https://www.itnewsafrica.com/2020/03/kenyan-kamiti-boys-fraudsters-are-cleaning-out-mobile-cash-wallets/.

[3] Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. Future Internet, 11(4), 89. 2019.

[4] Muia, J. Woman Conned Ksh.800k By Inmate Who Promised Her State House HR Job. Citizen Digital. February 2022. https://www.citizen.digital/news/woman-conned-ksh800k-by-inmate-who-promised-her-state-house-hr-job-n292354.

[5] Kenya Law. COMPUTER MISUSE AND CYBERCRIMES. May 18 2018. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018.

[6] Directorate of Criminal Investigations. DIGITAL FORENSIC LABORATORY(DFL). https://www.cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html.

[7] Okubasu, D. Police Spokesperson Speaks After Citizen TV Exposes Kamiti Call Center. Kenyans.co.ke. April 2022. https://www.kenyans.co.ke/news/74894-police-spokesperson-speaks-after-citizen-tv-exposes-kamiti-call-center.