ANCIR iLab

# Covid-19 Lockdown Relief Package Scam

How users in African countries are scammed into sharing their banking information during the Covid-19 lockdown period

**07 / 2020**

# Covid-19 Lockdown Relief Package Scam

## TABLE OF CONTENTS

# The Authors

Code for Africa (CfA) is the continent's largest network of non-profit independent civic technology and open data laboratories, with teams of full-time technologists and analysts in 13 African countries. CfA's laboratories build digital democracy solutions that give citizens unfettered access to actionable information to improve citizens' ability to make informed decisions, and to strengthen civic engagement for improved public governance and accountability.

The African Network of Centres for Investigative Reporting (ANCIR) is a CfA initiative that brings together the continent's best investigative newsrooms, ranging from large traditional mainstream media to smaller specialist units. ANCIR member newsrooms investigate crooked politicians, organised crime and big business. The iLAB is ANCIR's in-house digital forensic team of data scientists and investigative specialists who spearhead investigations that individual newsrooms are unable to tackle on their own. This includes forensic analysis of suspected digital disinformation campaigns aimed at misleading citizens or triggering social discord or polarisation using hate speech or radicalisation or other techniques.

The iLAB subscribes to CfA's guiding principles:

1. **We show what's possible.** Digital democracy can be expensive. We seek to be a catalyst by lowering the political risk of experimentation by creating successful proofs-of-concept for liberating civic data, for building enabling technologies and for pioneering sustainable revenue models. We also seek to lower the financial costs for technology experimentation by creating and managing 'shared' backbone civic technology and by availing resources for rapid innovation.
2. **We empower citizens.** Empowering citizens is central to our theory of change. Strong democracies rely on engaged citizens who have actionable information and easy-to-use channels for making their will known. We therefore work primarily with citizen organisations and civic watchdogs, including the media. We also support government and social enterprises to develop their capacity to meaningfully respond to citizens and to effectively collaborate with citizens.
3. **We are action oriented.** African societies are asymmetric. The balance of power rests with governments and corporate institutions, at the expense of citizens. Citizens are treated as passive recipients of consultation or services. We seek to change this by focusing on actionable data and action-orientated tools that give 'agency' to citizens.
4. **We operate in public.** We promote openness in our work and in the work of our partners. All of our digital tools are open source and all our information is open data. We actively encourage documentation, sharing, collaboration, and reuse of both our own tools, programmes, and processes, as well as those of partners.
5. **We help build ecosystems.** We actively marshal resources to support the growth of a pan-African ecosystem of civic technologists. Whenever possible we reuse existing tools, standards and platforms, encouraging integration and extension. We operate as a pan-African federation of organisations who are active members of a global community, leveraging each other's knowledge and resources, because all of our work is better if we are all connected.

This report was authored by the iLAB's East African team, consisting of investigative manager Allan Cheboi, data analyst Jean Githae, data technologist Robin Kiplangat and datavis designer Odhiambo Ouma . The report was edited by senior programme manager Amanda Strydom and deputy CEO Chris Roper, and approved for publication by CEO Justin Arenstein.

CODE for AFRICA

DW Akademie

# Glossary

Detailed descriptions and explanations of terms and abbreviations relevant to this report are listed below. These descriptions and explanations serve to clarify the usage in our report and are not intended to to be authoritative.

| Abbreviation | Description |
|---|---|
| ANCIR | African Network of Centres for Investigative Reporting |
| CfA | Code for Africa |
| CIB | Coordinated Inauthentic Behaviour |
| Covid-19 | Coronavirus disease of 2019 |
| EGP | Egyptian pounds |
| GH¢ | Ghananian cedi |
| Kshs | Kenyan shillings |
| N | Nigerian Naira |
| R | South African Rand |
| Rs | Indian rupee |
| SEO | Search Engine Optimization |
| UGX | Ugandan shillings |

# Executive Summary

Covid-19 lockdown relief package scam: How users in African countries are scammed into sharing banking information during the Covid-19 lockdown period

WhatsApp, owned by Facebook, is one of the most popular instant messaging apps globally, with over 1.5 billion monthly active users. It is widely used across Asia, Africa, Latin America, and Europe. But increasingly, WhatsApp has also been documented as a leading factor in propagation of disinformation, misinformation and political propaganda. At the same time, because it is an end-to-end encrypted platform, WhatsApp cannot access or see content being shared by users, so the general view is that there is very little that can be done.

Constant monitoring of content shared on WhatsApp by researchers helps with identification of malicious practices before the majority of citizens fall victim to threat actors. The research publications can further be used in creating awareness, and enhancing public knowledge in the fight against disinformation and coordinated inauthentic behaviour.

With nationwide lockdown in effect across a number of African countries, and the economic downturn seen all over the world, the crisis has had a substantial impact on many people's livelihoods. Several governments have been disbursing money in attempts to alleviate the living conditions of low-income or unemployed citizens during the Covid-19 epidemic.

According to CitizenTV, a Kenyan media company, Kenya's government has been providing a weekly stipend of Ksh.1,000 to vulnerable households. Dr. Karanja Kibicho, Interior Ministry Principal Secretary, told CitizenTV that the government had identified 108,000 households in Nairobi, Mombasa, Kwale and Kilifi counties, who have since received the money following the programme's roll-out. Speaking in an interview on Inooro FM, he said during the first disbursement that each of the 108,000 households received Ksh 2,000 and the amount is expected to feed them for a two-week period.

Scammers have taken advantage of the epidemic to conduct malicious activities targeting unsuspecting citizens of different countries.

CfA identified a case where perpetrators targeted users from African countries such as Kenya, South Africa, Uganda, Nigeria, Egypt and Ghana with a digital campaign intended to harvest their banking information. The campaign falsely presented a Covid-19 "relief package" from the government. In reality, it enticed WhatsApp users to not only share the campaign with several of their WhatsApp contacts, but also willingly share their banking information that could be used for further social engineering attacks and financial crime.

Unique to this investigation, the perpetrators used fake profiles and web-pages on Blogger, a blog-publishing service bought by Google in 2003. In previous investigations, perpetrators created and registered personal websites used to run such scams.

A CfA investigation analysed the source code of the associated blog sites, which revealed the links to three blog profiles. The blog profiles had no personally identifiable information and a reverse image

search for one of the profile's pictures showed it was a fake ID that had been used prolifically across social media, blogs and review platforms.

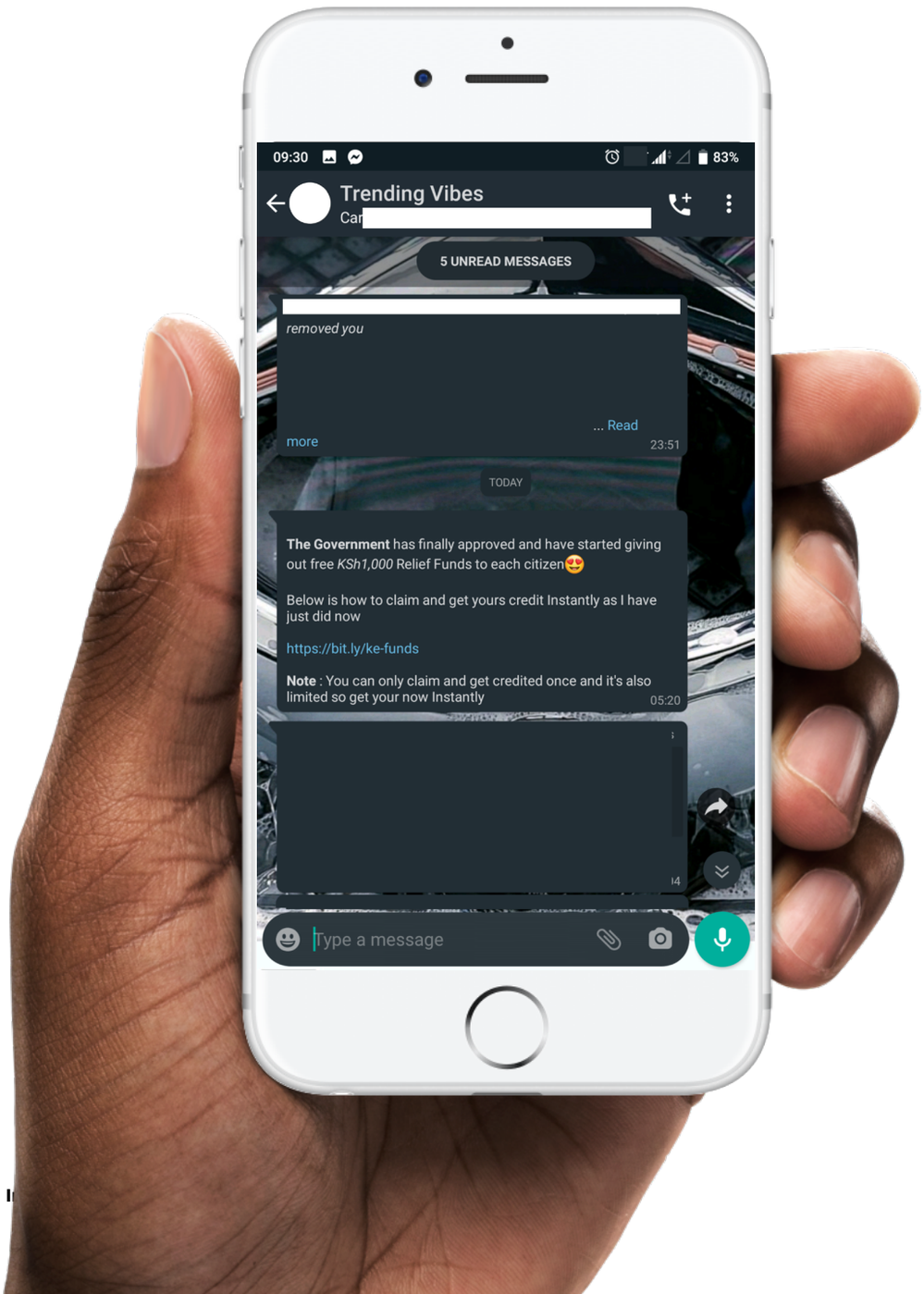
The main perpetrator created the blog profile in April 2020, a month after many governments in Africa imposed curfew and lockdowns in the respective countries. The campaign used the WhatsApp chain-messaging strategy to propagate the intended scam targeting multiple African countries. Blogs customised to Kenya, South Africa, Nigeria, Ghana, Egypt and Uganda were used to deceive users into sharing their banking information with the threat actors.

Independent fact checkers have debunked a number of claims related to the network of blogs used in the campaign under investigation and found them to be FALSE. Facebook has also flagged posts using urls pointing to the blog-pages as false information.

# The Campaign Mechanics

The campaign was spread mainly via a short WhatsApp message that contained a link to one of the blogs created by the main perpetrator, only identified as 'Fred'. The message was shared to users depending on the country of origin and the links were pointing to the specific blogs created for each country.

This message was deceptively styled to give the impression that each government was giving away money as part of a coronavirus relief package programme. Once a user clicked on this link, a two-staged process commenced.

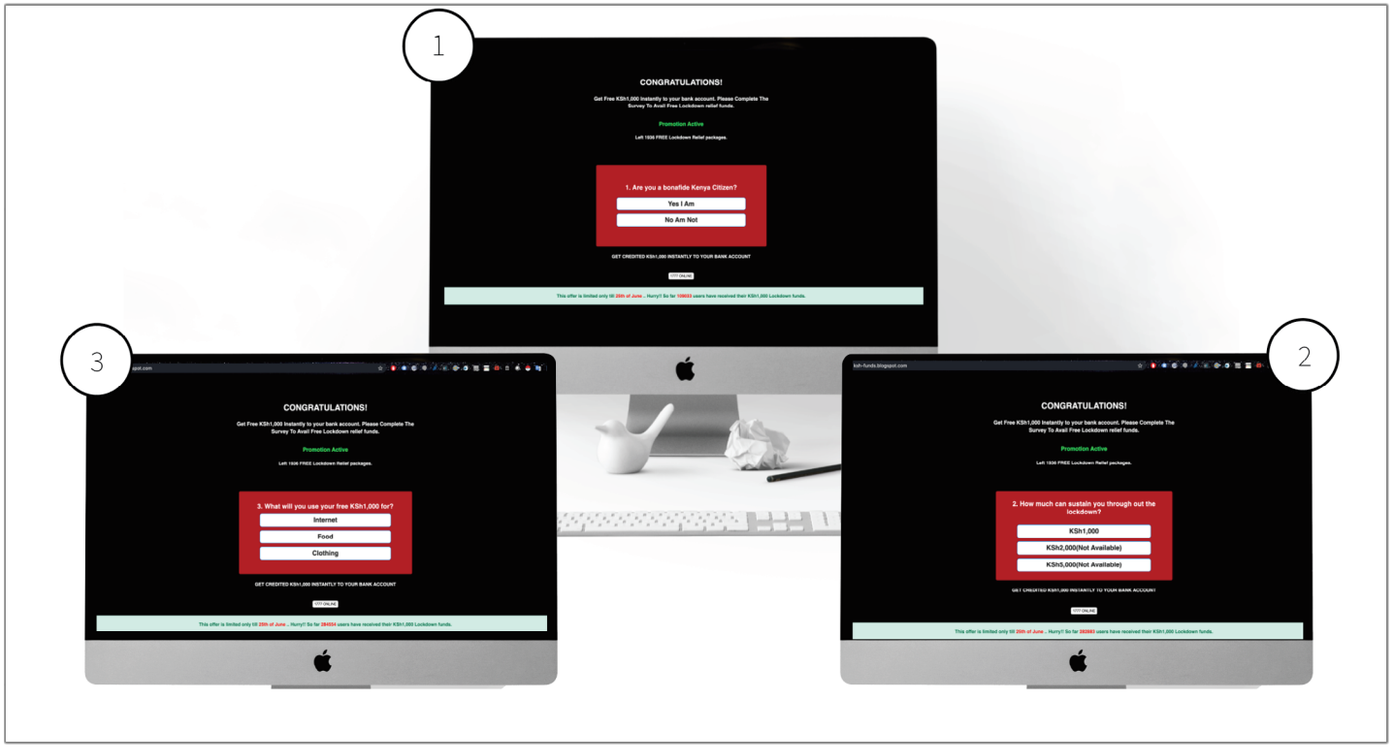



**A screengrab of the WhatsApp message linking to the dubious blogs, indicating the deceptive relief package from the government (Source: CfA)**

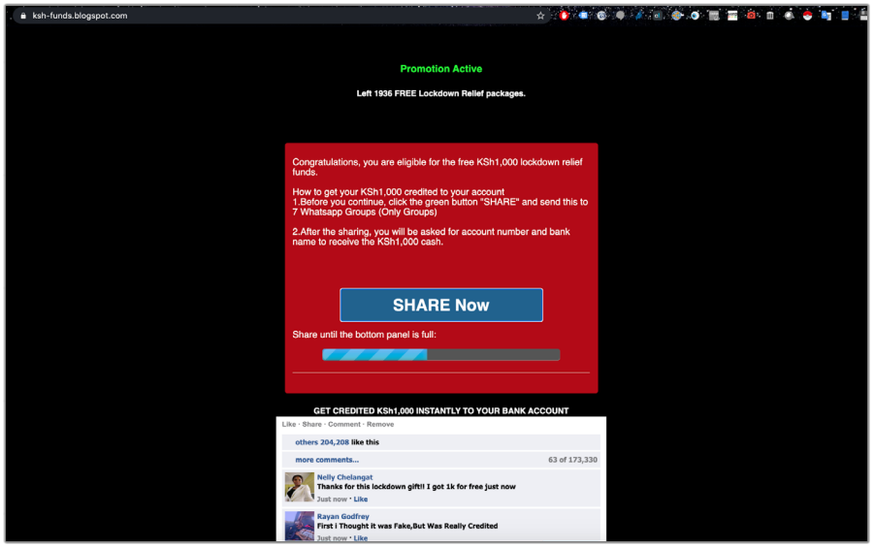
## The fake blog landing page

Firstly, a landing page (http://ksh-funds.blogspot.com/ archive) enticed the user to take a short survey with the following questions:

1. Are you a bonafide Kenyan Citizen?
2. How much can sustain you throughout the lockdown?
3. What will you use your free Kshs 1,000 for?

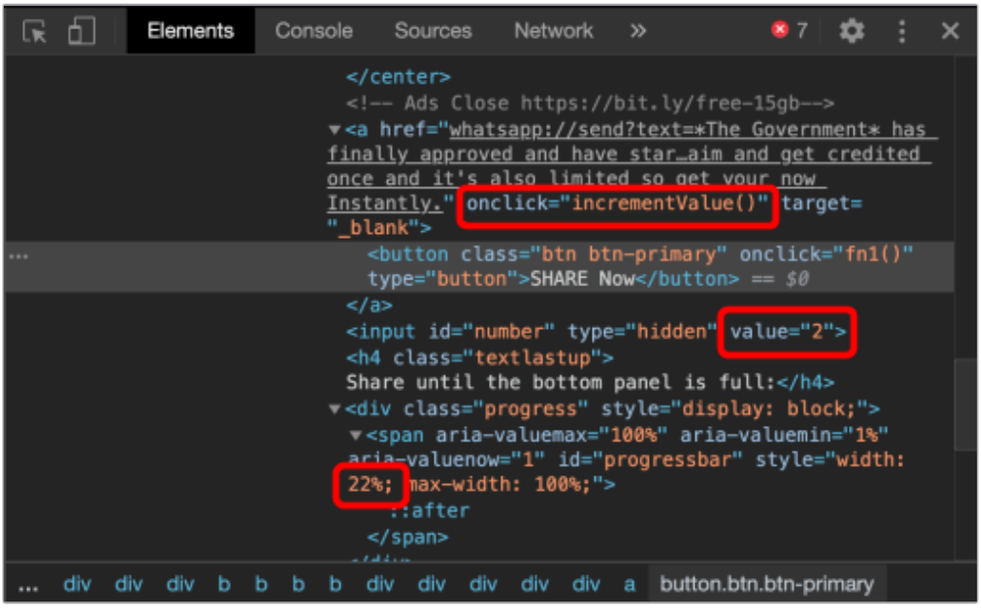



Once the user answers the survey questions, they are prompted to share the link to at least seven WhatsApp groups. A progress bar would keep track of the number of times a user shared it with their friends or groups

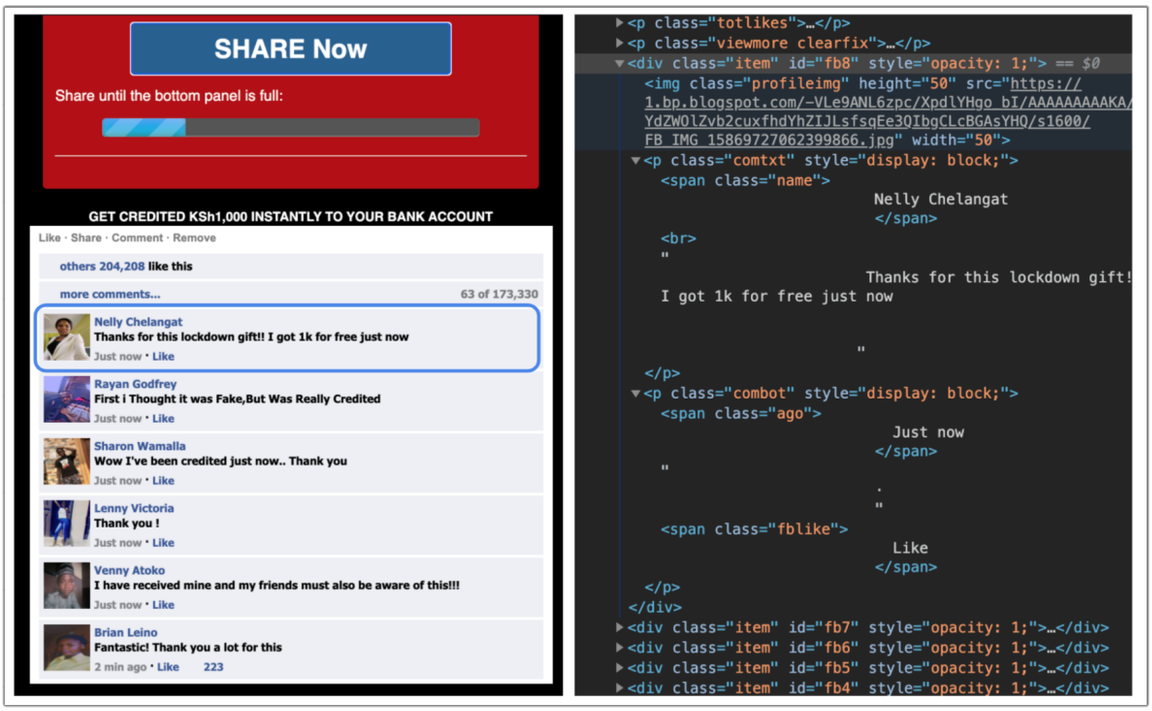



**A screengrab taken on 6 July 2020 from the source code of the page revealing the functions called when clicking the 'Share Now' button (Source: CfA)**

These steps could be discerned from the JavaScript functions embedded into the buttons.

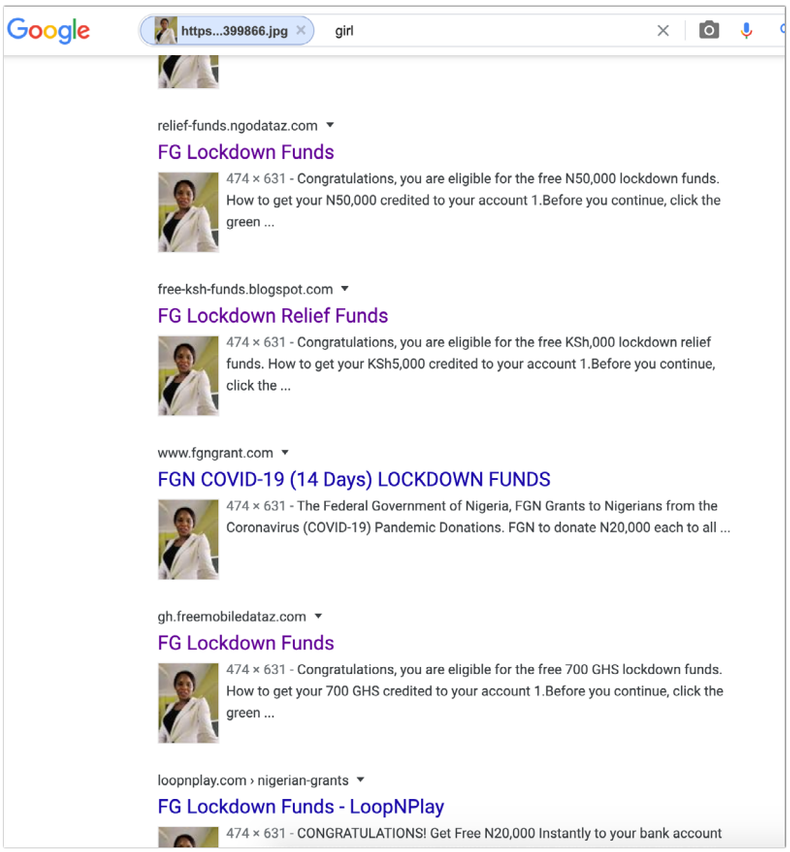



Clicking the "Share now" button (blue) pre-drafted a WhatsApp message to be forwarded to several WhatsApp Groups. This would also prompt the function "onlick="incrementaValue( )" which would increase the value to "2". This leads to an increase in the width of the progress bar by 11% as shown in the screengrab below. This process ensured that users propagated the website to several of their WhatsApp contacts before they were able to claim the fake lockdown relief package. We further noted that there was a fake Facebook comments section below the 'Share Now' button used to convince users of previous award claims.



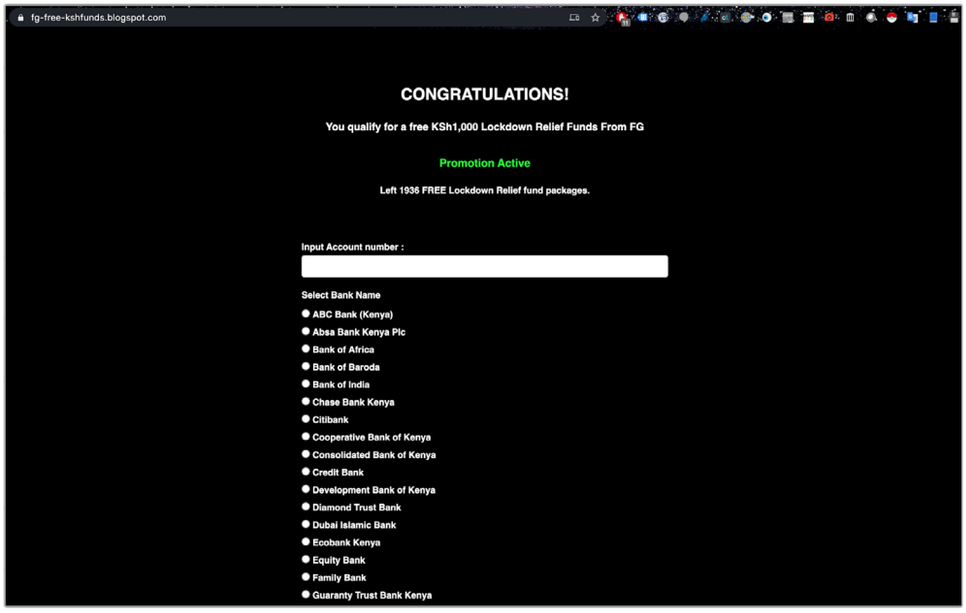

**Screengrabs taken on 6 July 2020 from the ksh-funds.blogspot.com (left) imitating a Facebook comments section, and the accompanying source code (right). (Source: @ archive/CfA)**

These comments were hard-coded, and reverse image search of the profile pictures revealed that scores of blogs running the same campaign used the same profile pictures. This enabled us to identify additional blogs linked to the campaign.

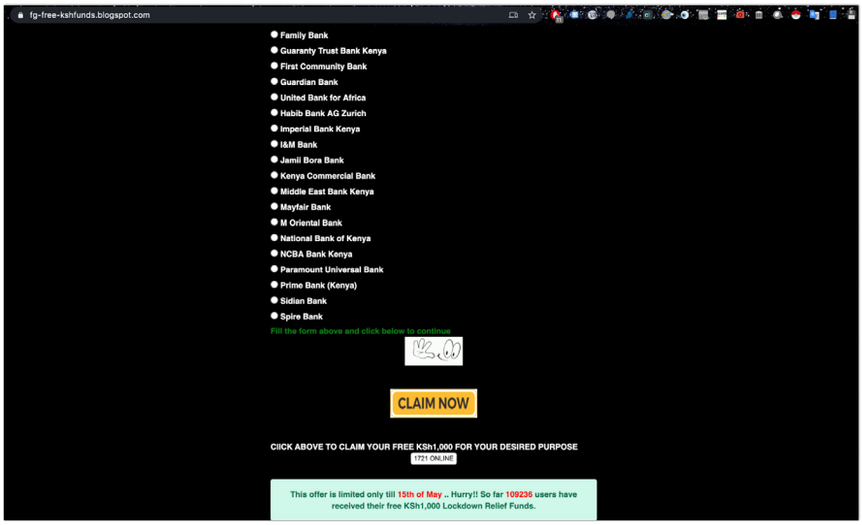



## The honey pot

Once the threshold is met (max-width; 100%), the user is redirected to a second site, https://fg-free-kshfunds.blogspot.com/archive, which we are referring to as the "honey pot". The user is prompted to enter their bank account number and select the bank name from the options listed below the text box.

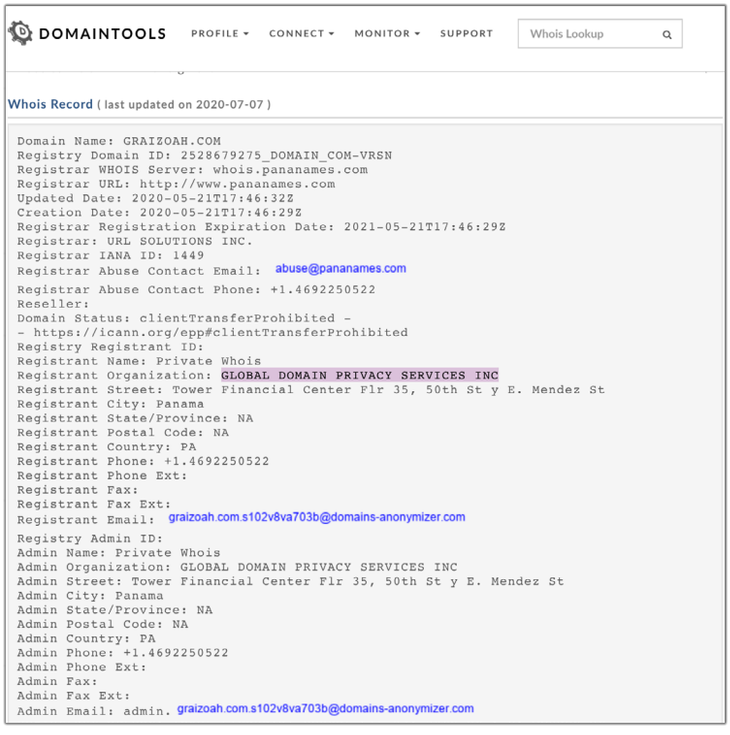


Once the user fills the required information, clicking on the “Claim Now” button redirects the user to the final webpage through a URLl as shown in the source code on the right.





The URL under the domain www.graizoah.com was registered on 21 May 2020 by an unknown entity through a private WHOIs service organisation based in Panama called Global Domain Privacy Services Inc. The registrar of the domain is URL Solutions Inc, a domain registration service provider also in Panama.

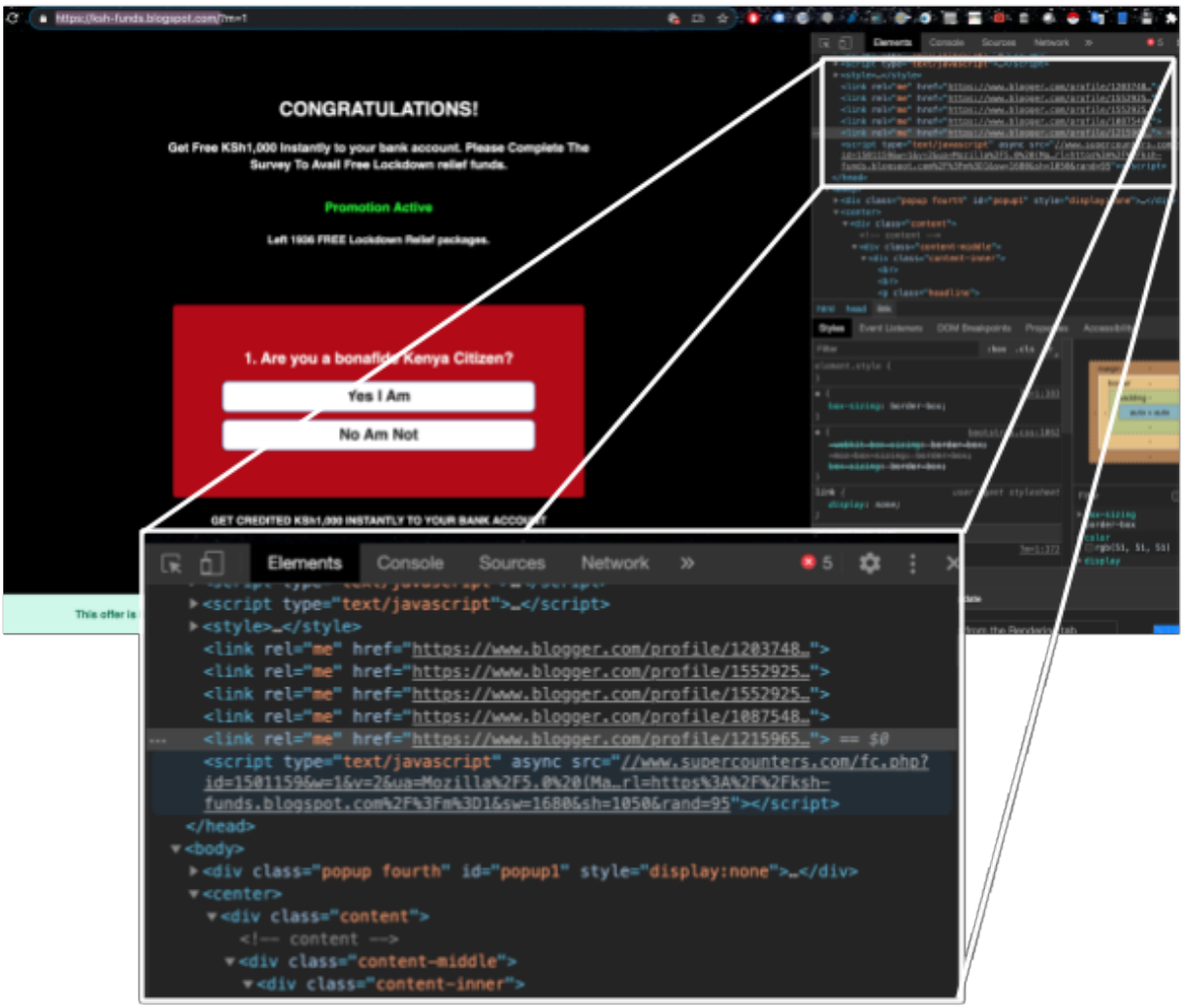




The url under this website redirects the user to https://www.gearbest.com/, an online shop registered in GuangDong province in China.

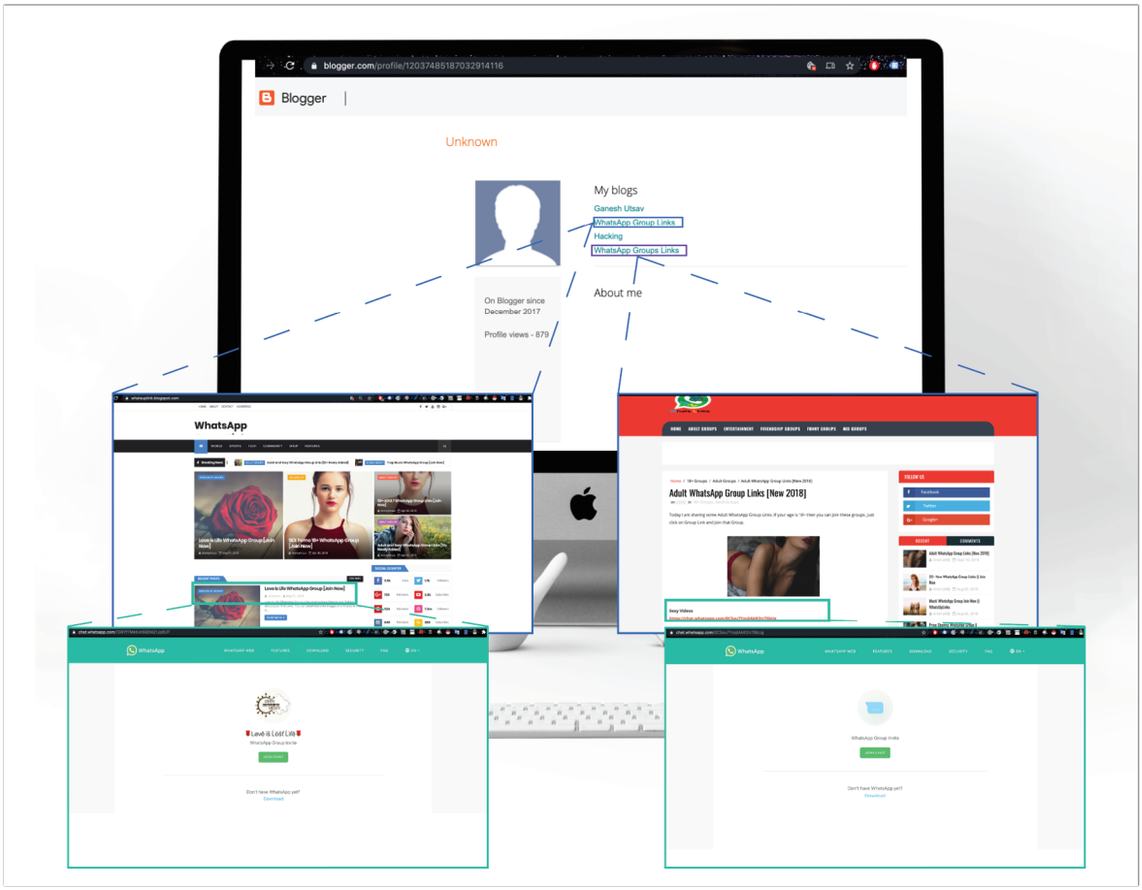
# The Perpetrators

A dive into the source code of the landing page http://ksh-funds.blogspot.com revealed the blogger profiles running the promotion. The header section of the blog-site showed a link to three profiles that were determined as fake accounts used to create and share the campaign.



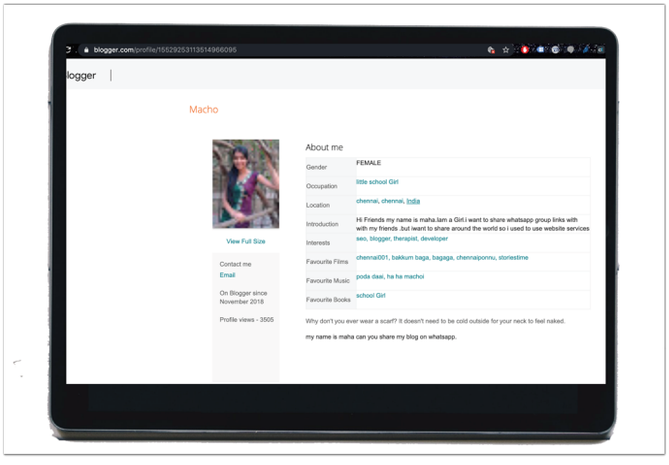
## Profile 1 : https://www.blogger.com/profile/12037485187032914116 - Archive

The profile with the name “Unknown” was created in December 2017 and had no profile picture. This indicates it was a fake profile created solely to run the linked blogs. CfA’s investigation identified two blogs that were directly run by the account specifically created to entice users to join WhatsApp groups. Most of the groups were tailored to share pornographic content.

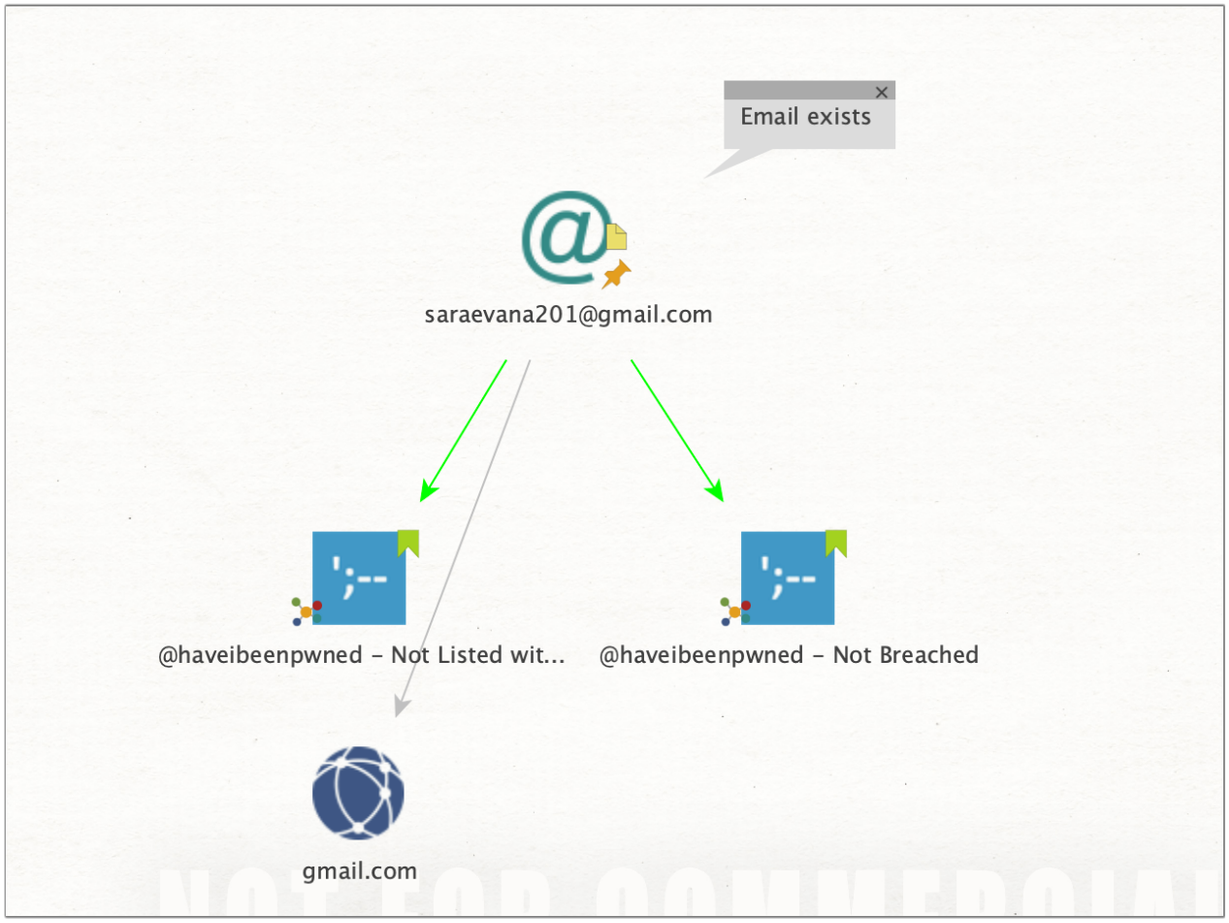


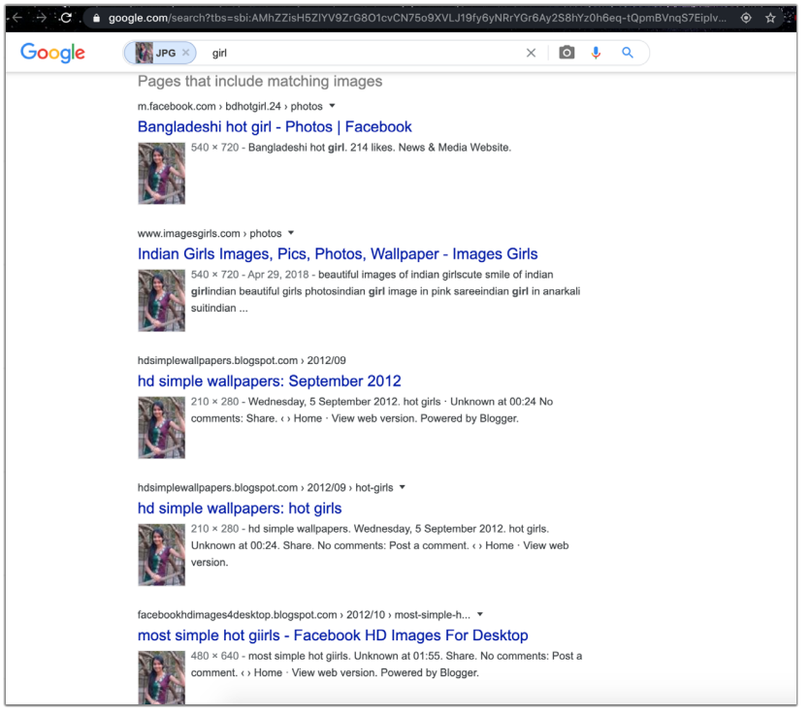

## Profile 2 : https://www.blogger.com/profile/15529253113514966095 - Archive

The profile with the name ‘Macho’ was created in November 2018. According to the profile information available, the administrator describes herself as Maha, is located in Chennai, India and has interests in blogging and SEO.



We identified an email address linked to the account 'saraevana201@gmail.com'. A search on Maltego revealed that the email address exists but did not yield further information about the ownership of the address.



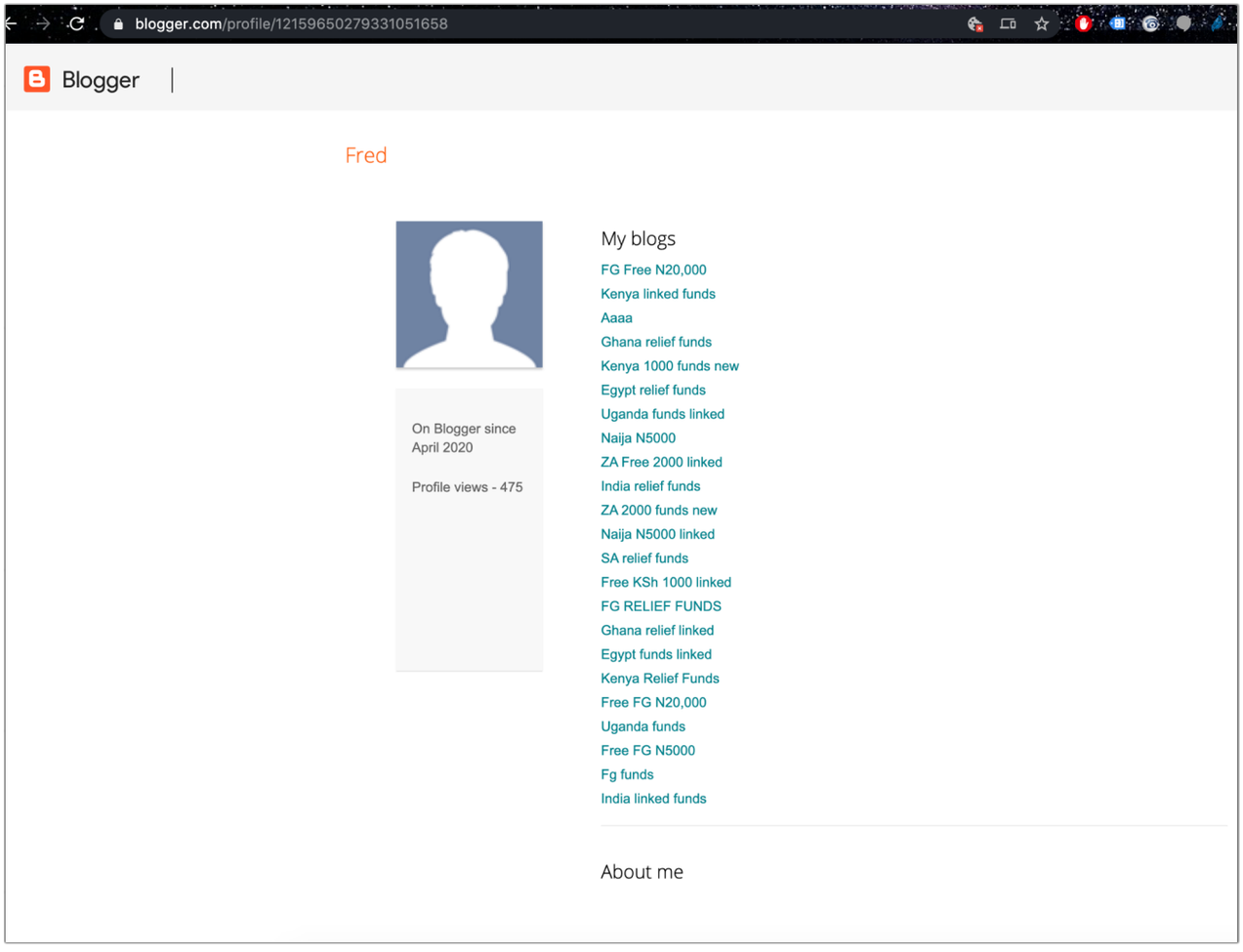

A reverse image search of the profile picture showed scores of websites used the same profile pictures.

This indicates that it was a fake profile created solely to share the campaign through associated WhatsApp groups and contacts.

## Profile 3 : https://www.blogger.com/profile/12159650279331051658 - Archive

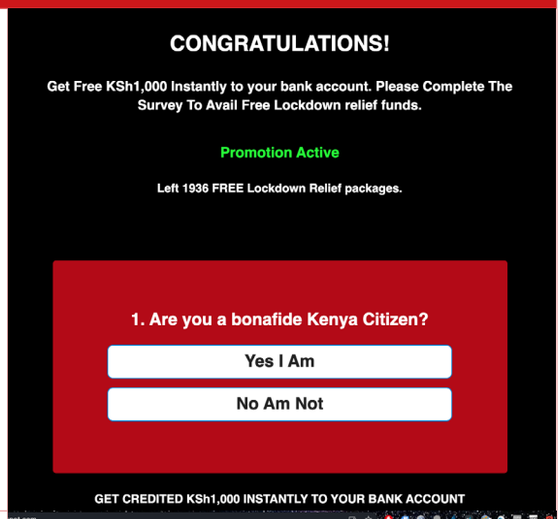
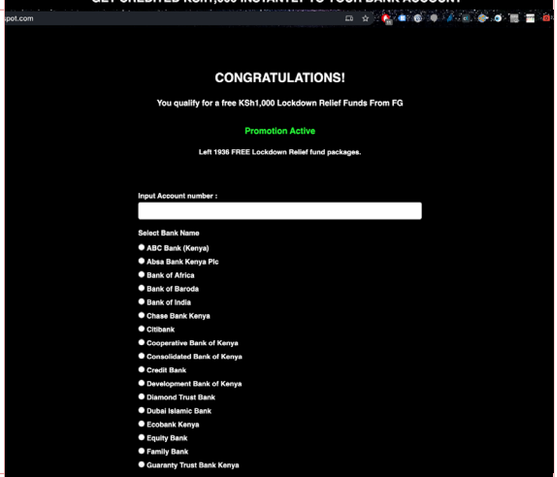
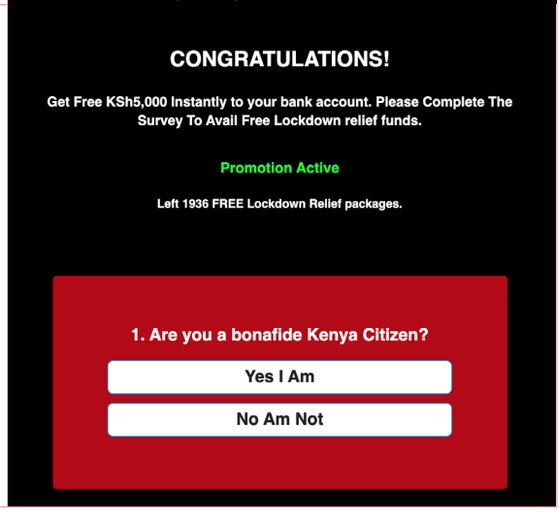
The profile named “Fred” was created in April 2020 and did not have any other identifiable information. This profile owned both the landing blog page and the honey pot page described in the campaign mechanics section.

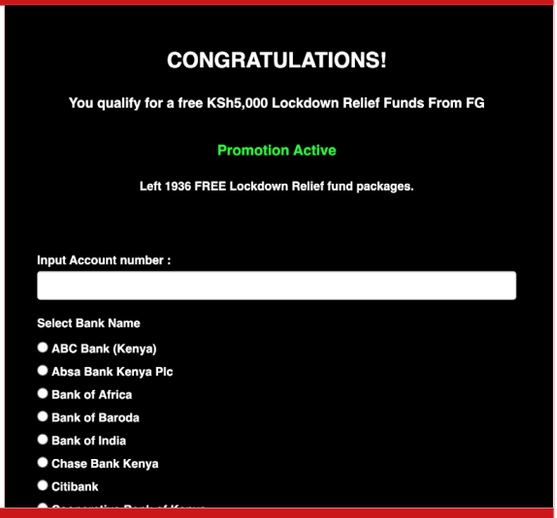
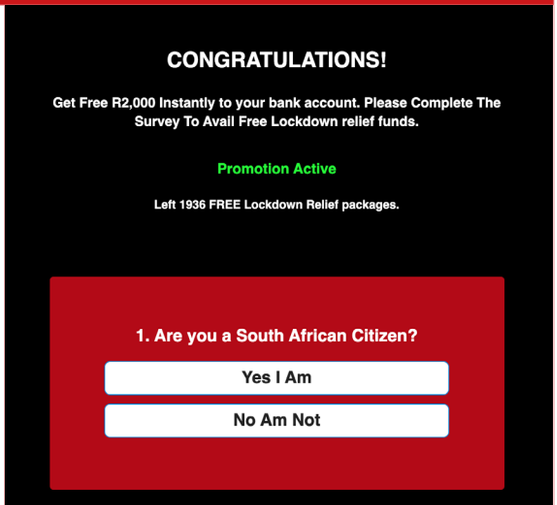
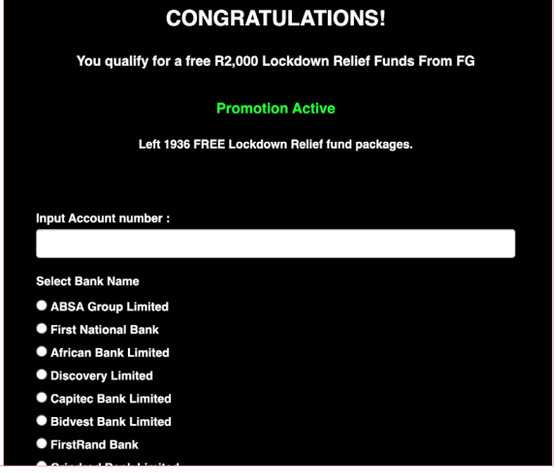
Further, the account also owned several blog pages linked to the same campaign in the other affected African countries. We also noted a blog page targeting Indian citizens with the same promotion.

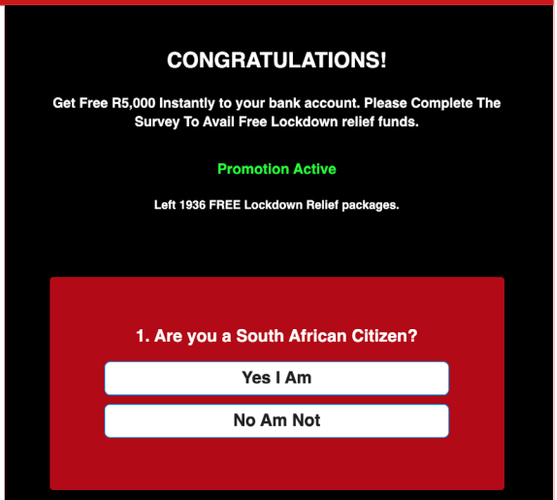
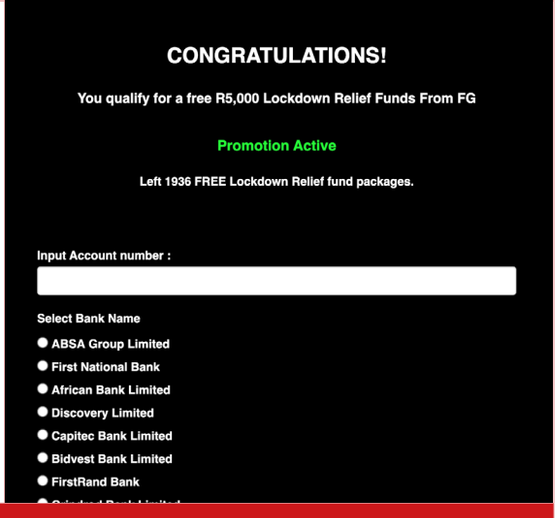
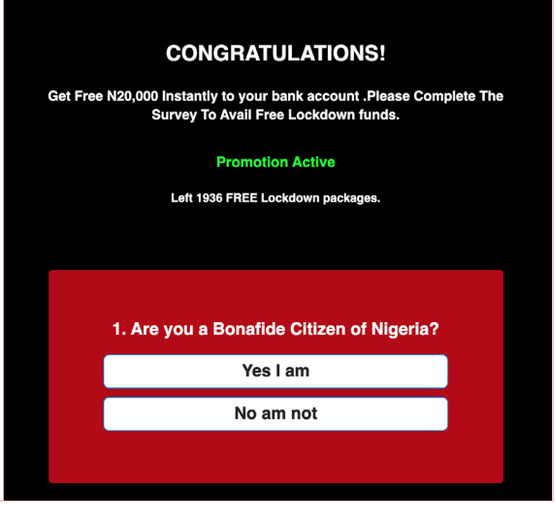


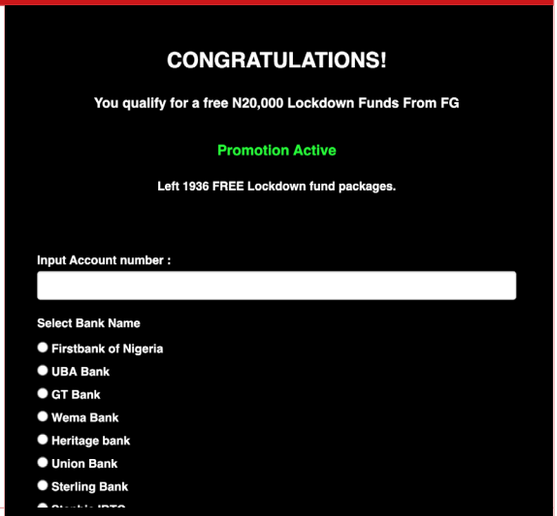
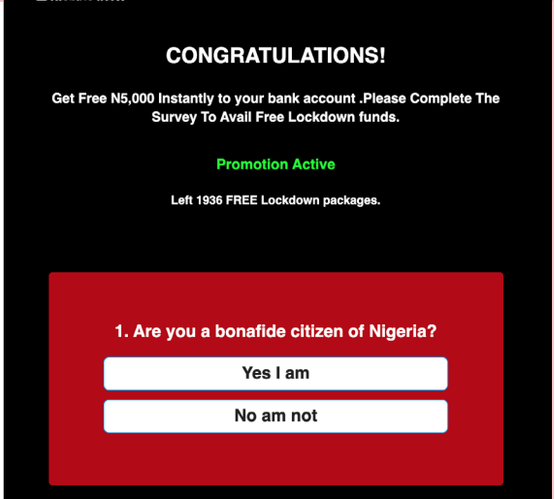
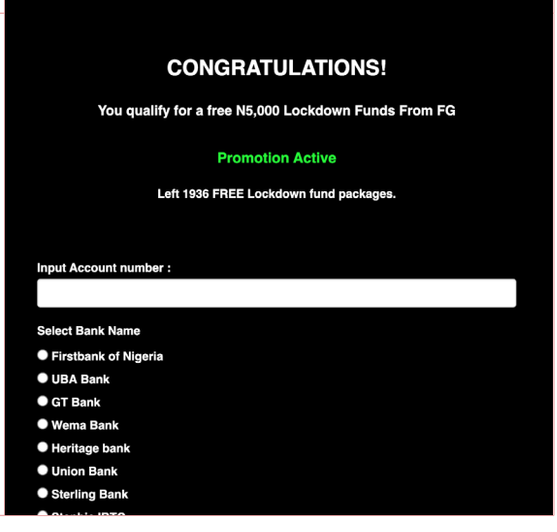

We noted that the pages created for the other countries were identical to the Kenya campaign scenario, except for a few customisations on the country name, currency, list of banks, and award amount. They also had the same campaign mechanics and were linked to the same perpetrator profiles.

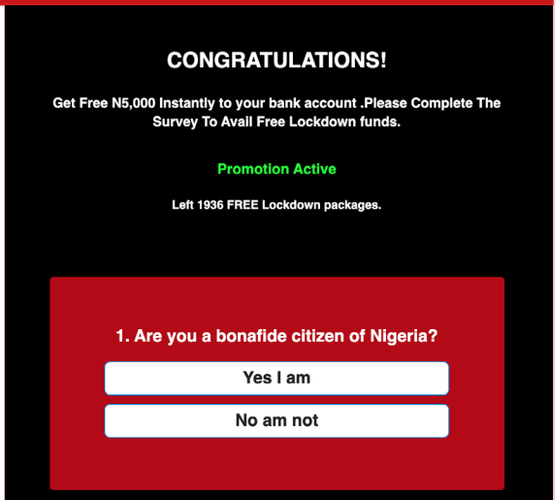
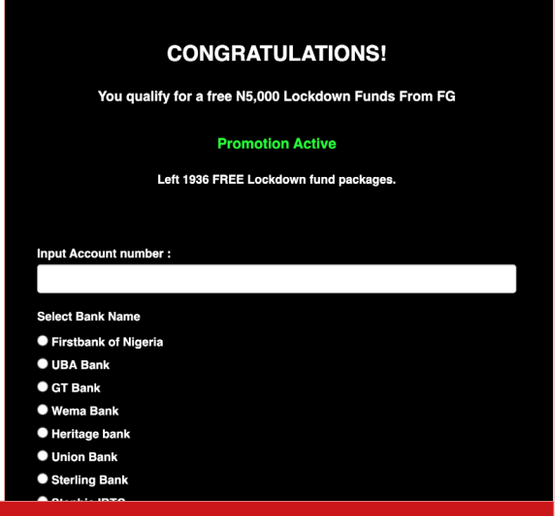
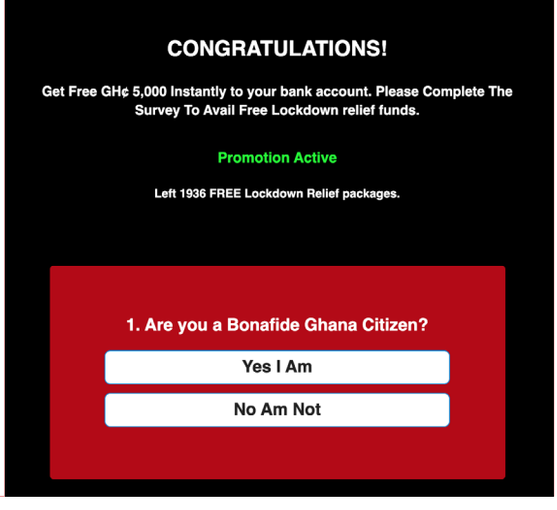
Below is a list of all campaigns under the profile:

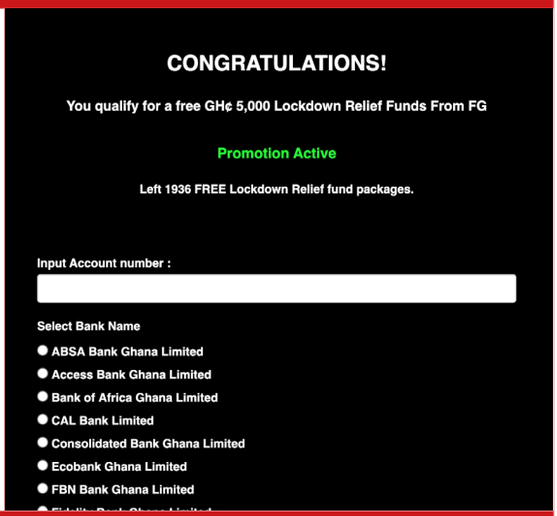
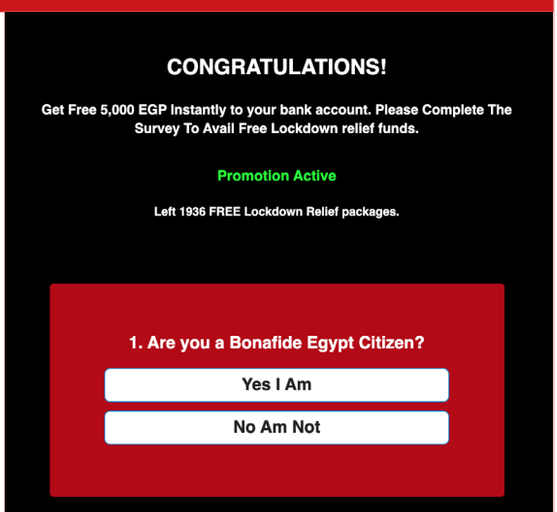
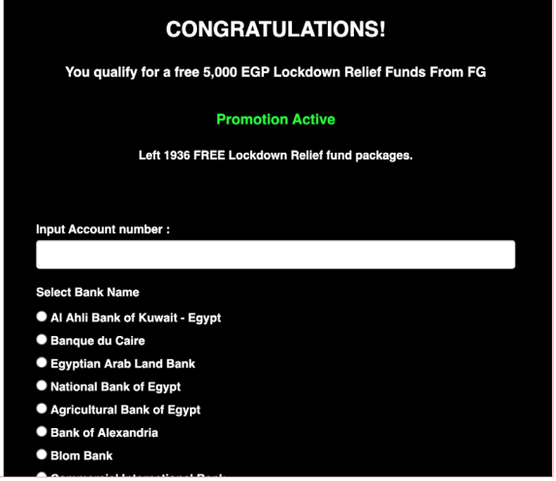
| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Kenya** | | | | |
| Landing Page | Kenya 1000 funds new | Kshs 1,000 | Link / Archive |   |
| Honey Pot | Free KSh 1000 linked | Kshs 1,000 | Link / Archive |   |
| Landing page | Kenya Relief Funds | Kshs 5,000 | Link / Archive |   |

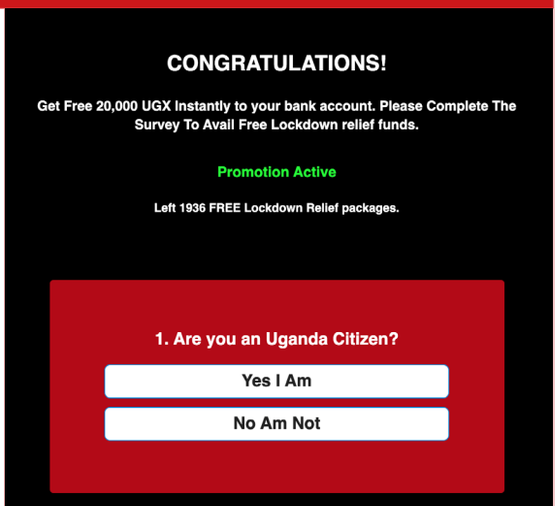
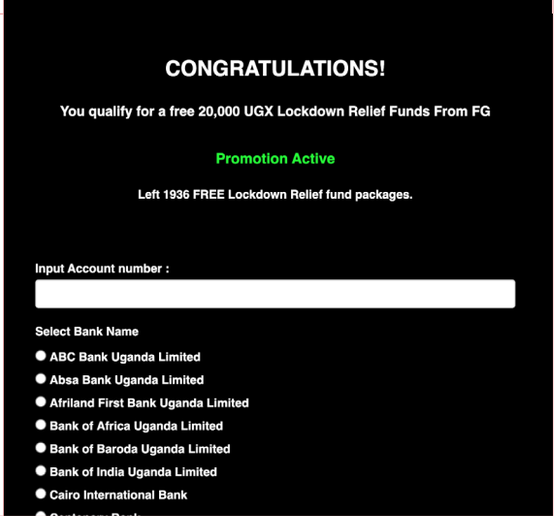
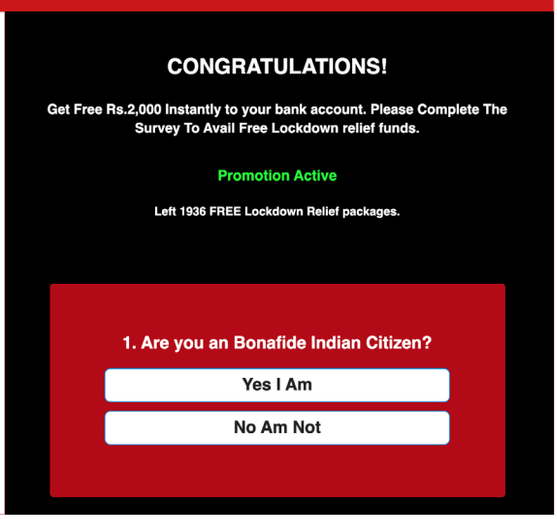
| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Kenya** | | | | |
| Honey Pot | Kenya linked funds | Kshs 5,000 | Link / Archive |  |
| **South Africa** | | | | |
| Landing Page | ZA 2000 funds new | R 2,000 | Link / Archive |  |
| Honey Pot | ZA Free 2000 linked | R 2,000 | Link / Archive |  |

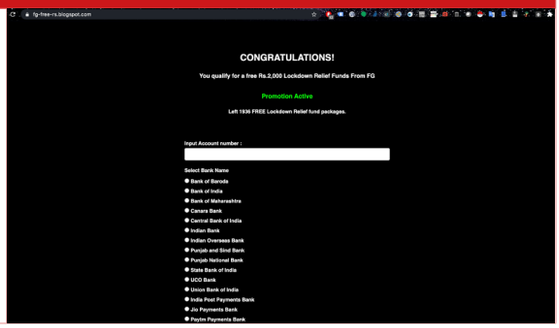
| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **South Africa** | | | | |
| Landing Page | FG RELIEF FUNDS | R 5,000 | Link / Archive |   |
| Honey pot | SA relief funds | R 5,000 | Link / Archive |   |
| **Nigeria** | | | | |
| Landing page | FG Free N20,000 | N 20,000 | Link / Archive |   |

| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Nigeria** | | | | |
| Honey pot | Free FG N20,000 | N 20,000 | Link / Archive |  |
| Landing page | Naija N5000 | N 5,000 | Link / Archive |  |
| Honey pot | Naija N5000 linked | N 5,000 | Link / Archive |  |

| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Nigeria** | | | | |
| Landing Page | FG Funds | N 5,000 | Link / Archive |   |
| Honey Pot | Free FG N5000 | N 5,000 | Link / Archive |   |
| **Ghana** | | | | |
| Landing Page | Ghana relief funds | GH¢ 5,000 | Link / Archive |   |

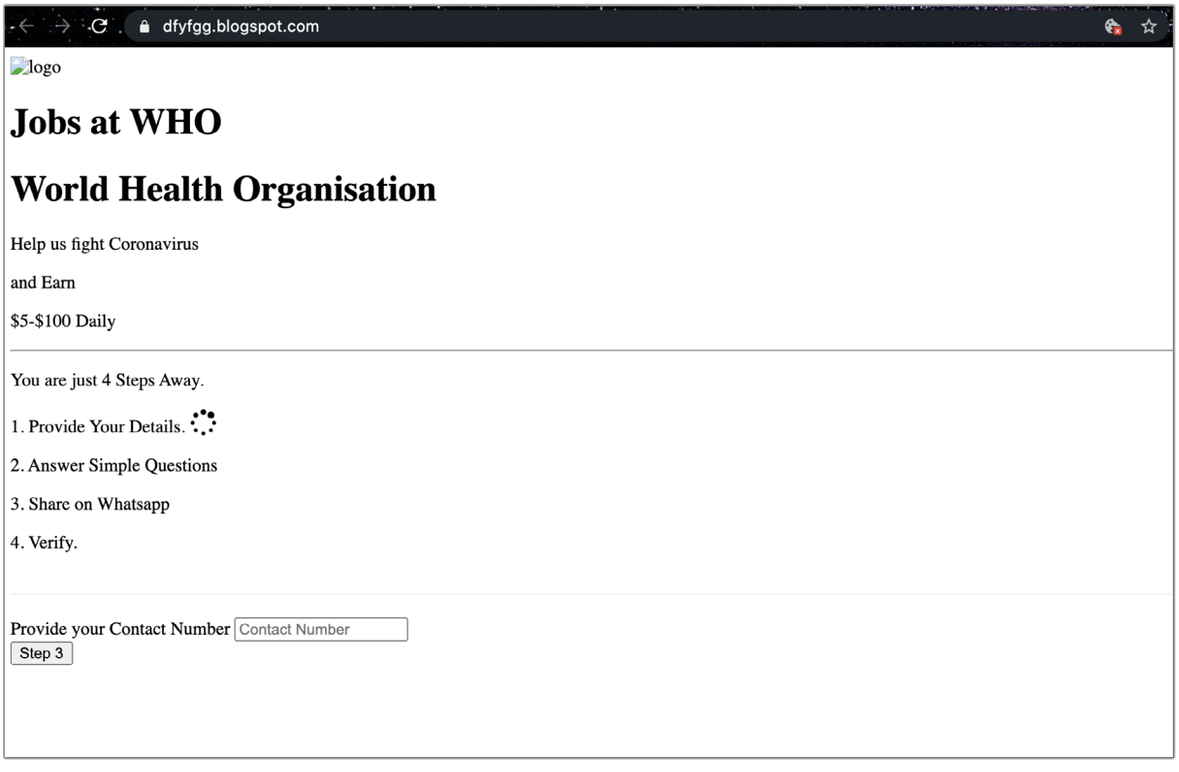
| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Ghana** | | | | |
| Honey Pot | Ghana relief linked | GH¢ 5,000 | Link / Archive |  |
| **Egypt** | | | | |
| Landing Page | Egypt Relief funds | EGP 5,000 | Link / Archive |  |
| Honey Pot | Egypt funds linked | EGP 5,000 | Link / Archive |  |

| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **Uganda** | | | | |
| Landing Page | Uganda funds | UGX 20,000 | Link / Archive |   |
| Honey pot | Uganda funds linked | UGX 20,000 | Link / Archive |   |
| **India** | | | | |
| Landing Page | India relief funds | Rs 2,000 | Link / Archive |   |

| Type | Blog Name | Amount | Blog Links | Image |
|---|---|---|---|---|
| **India** | | | | |
| Honey Pot | India Linked funds | Rs 2,000 | Link / Archive |  |



CfA also identified a different, unfinished blog site among the list of blogs with a different campaign titled "Jobs at WHO - World Health Organisation". The blog page titled 'Aaaa' under the url https://dfyfgg.blogspot.com/ Archive seems to be a draft of a future campaign the perpetrators plan on running.

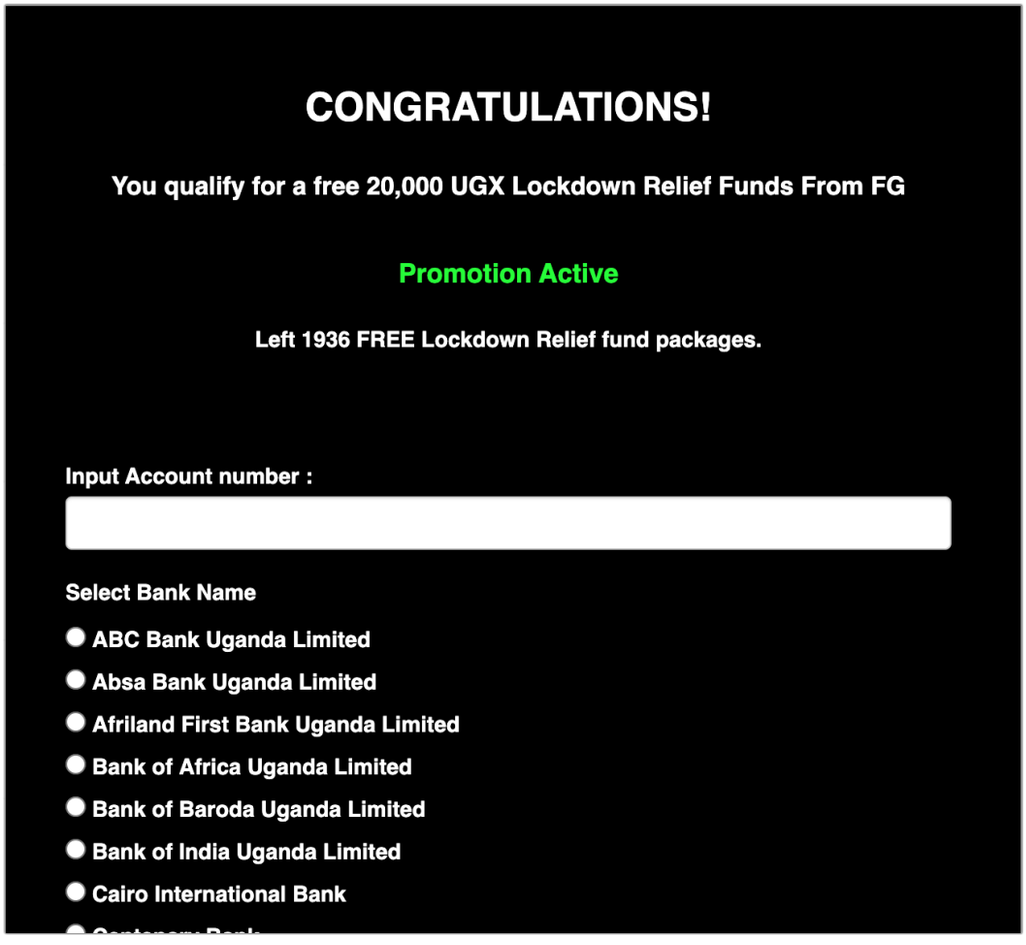


# Amplification

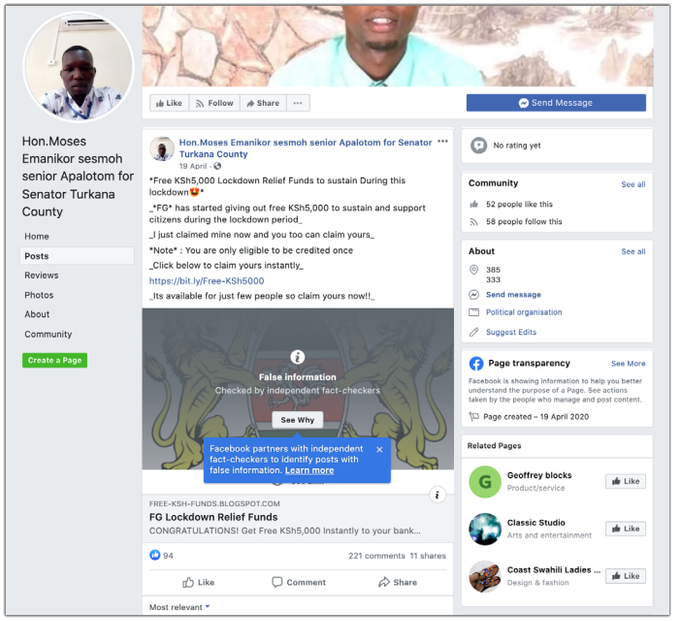
We reviewed the composition of the pre-drafted message used to share the campaign on WhatsApp and saw that the URLs for the landing pages used in the campaign had been masked using Bitly, a URL shortening service. A back-link search of the shortened URLs enabled us to identify cases where the campaign was shared on both Facebook and Twitter.

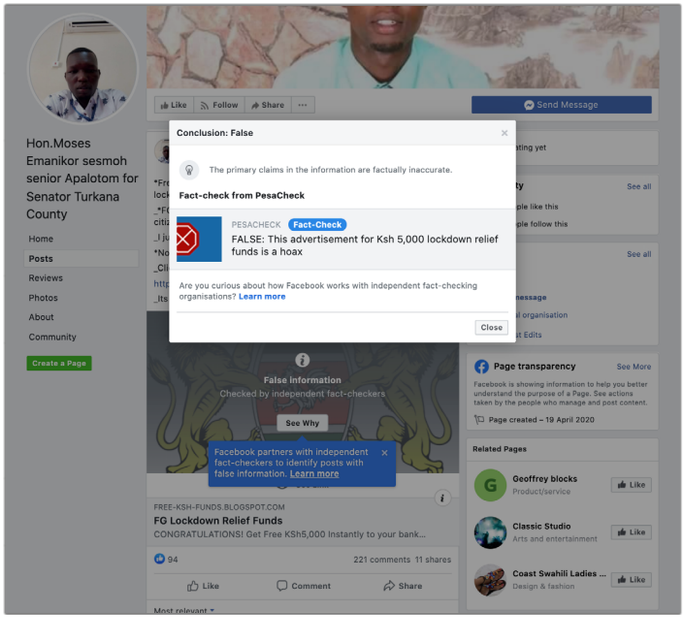
## Facebook

Using CrowdTangle, we identified 11 cases where the campaign URLs had been shared on Facebook groups and pages.



Notably, a post shared on Facebook page titled "Hon.Moses Emanikor sesmoh senior Apalotom for Senator Turkana County" had been flagged and fact-checked by PesaCheck, an independent fact-checking team, incubated by the same umbrella organisation that incubates the iLAB, and found it to be FALSE. Facebook has since flagged the post as false information.

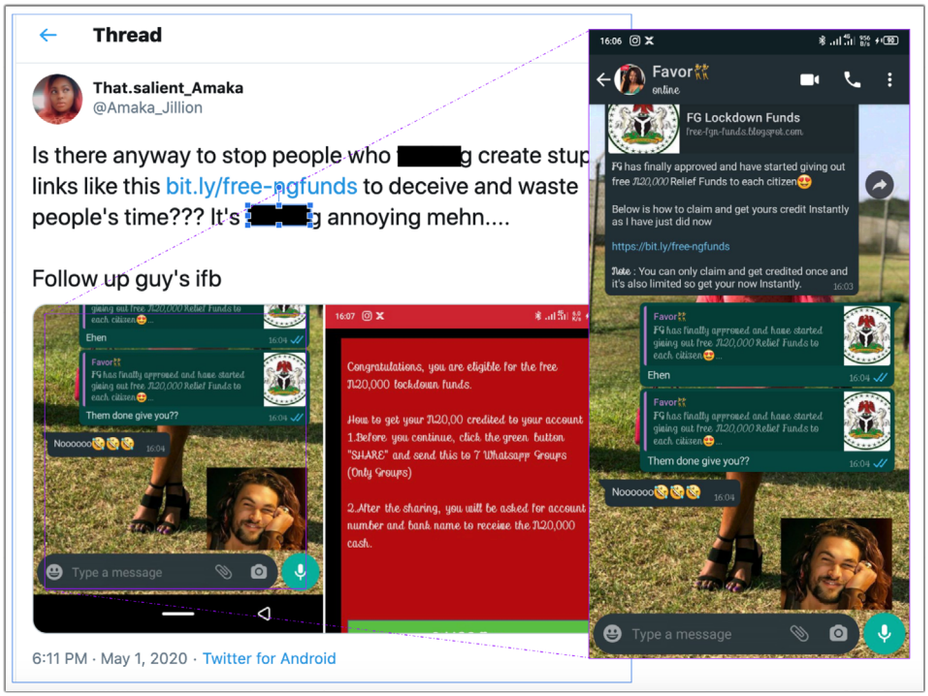



## Twitter

Using Twitter search functionality, we identified 15 cases where the campaign URLs had been shared on Twitter. Most of the posts were tweeted by concerned citizens either warning the public or seeking clarifications on whether the campaign was genuine.

Notably, Twitter user @Amaka_Jillion based in Lagos, Nigeria had received a WhatsApp text with information to participate in the lockdown package relief campaign.



# Conclusion

With nationwide lockdown in effect across a number of African countries, and the economic downturn seen all over the world, the crisis has had a substantial impact on many people's livelihoods. Several governments have been disbursing money in attempts to alleviate the living conditions of low-income or unemployed citizens during the Covid-19 epidemic.

The scammers' angle of attack has shifted from the traditional voucher-based scams to the use of Covid-19 relief package narratives to dupe citizens into sharing personal and banking information which can be used in malicious ways to the detriment of the victims.

The attack being run from a different country demonstrates coordinated inauthentic behaviour by the perpetrators to deceive citizens in other countries. This is categorised as disinformation and social media platforms, civic watchdog organisations and media houses are required to increase their efforts in fighting such practices.

# Recommendations

## We recommend that:

1. Naming and shaming individuals and organisations that create/share deceptive campaigns should be a priority for media, watchdog organisations and government institutions. iLAB is committed to exposing perpetrators who feed on people's illiteracy, gullibility and fear;
2. Self-publishing platforms such as Blogger, SquareSpace, etc should create hotlines for mis/disinformation researchers and investigators to flag suspected coordinated inauthentic behaviour. Further, once content has been confirmed as false or used to propagate deceptive behaviour, they should either be tagged, blocked or deleted from the platforms. iLAB has since shared with Google a recommendation to further investigate activities of the accounts identified during this investigation and take action;
3. Newsrooms should put in place measures to not only fact-check, but conduct investigations to identify perpetrators of such practices. iLAB has developed a database of sockpuppet accounts identified in various investigations. The database is continuously updated and is available to credible partners. We further recommend that a central database should be created for investigators to better map and track the hidden syndicates behind disinformation campaigns.
4. Newsrooms and media organisations should create awareness of the existence of such scams and campaigns being run by malicious actors. iLAB has partnered with a number of Kenyan newsrooms to share results of such investigative findings with the general public. We are open to establishing additional partnerships with other newsrooms and media organisations to help in further creating awareness in the fight against disinformation.

## Published by

Code for Africa is the continent's largest federation of civic technology and data journalism labs with teams in: Burundi, Ethiopia, Ghana, Kenya, Morocco, Mali, Nigeer, Nigeria, Senegal, Sierra Leone, South Africa, Tanzania, Tunisia & Uganda

CfA Secretariat: 112 Loop Street, Cape Town, Western Cape, 8000, South Africa.
South Africa NPO Number 168-092 | Kenya NPO Number CPR/2016/220101 | Nigeria NPO Number: RC-1503312
Kenya Lab: Nairobi Garage, 8th Floor, Pinetree Plaza, Kaburu Drive, Nairobi, Kenya.
Nigeria (Abuja) Lab: Ventures Park, 29,Mambilla Street, Aso Drive, Abuja, Nigeria.
Nigeria(Lagos) Lab: Workstation, No 7, Ibiyinka Olorunbe street, off Saka Tinibu, Victoria Island, Lagos, Nigeria
Tanzania Lab: 7th Floor, 38 Tanzanite, Park, New Bagamoyo Road, Dar es Salaam, Tanzania.
Uganda Lab Pollicy, Plot 7 Kulubya Road, Bugolobi, Kampala, Uganda.

CODE for AFRICA

DW Akademie