ANCIR iLab

Free Internet Scam

How purported access to data bundles is used as a monetisation scheme that relies on racking up fake ad clicks.

08 / 2020

Free Internet Scam

TABLE OF CONTENTS

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
SEO	Search Engine Optimization
Kshs	Kenyan shillings

Executive Summary

Free internet scam: How purported access to data bundles is used as a monetisation scheme that relies on racking up fake ad clicks

During the Covid-19 pandemic period, access to the internet has been a critical asset in facilitating access to information and entertainment, and for individuals who were capable of working online. When a message offering free mobile data pops up on a messaging app such as WhatsApp, it may be tempting to unsuspecting users unaware of the existence of such scams.

In August 2020, CfA's iLab identified a fraudulent message being shared on WhatsApp, a messaging application owned by Facebook. The message read "*You can now get a free internet bundle of 50GB (All Networks) valid for 90days in Celebration of WhatsApp Anniversary*".
This in itself is not unusual as companies occasionally run promotional campaigns offering gift packages to users when celebrating major milestones or events. However, this promotion was found to be strikingly suspicious.

A CfA analysis determined that the message was not from WhatsApp, neither was the mobile data offer genuine, but was in fact a ploy to lure unsuspecting users.
WhatsApp is used by more than 2 billion people in more than 180 countries. This encourages cybercrooks to create schemes that could easily exploit the high volumes of users who could click on any of the fraudulent links shared.

The scam is set up to primarily spread via WhatsApp groups through a chain messaging strategy and is made to appear as if it's received from a friend who has claimed it and therefore recommends the offer.

The message shared has an attached link and if the user clicks on it, they are directed to a landing page with a WhatsApp logo, a bright counter showing the offer is close to expiry, and simple steps on how to claim the offer - accessed by completing a survey.

Scammers aim to get users to click on the link to fraudulently redirect them to web pages bearing ads, allowing perpetrators to generate revenue from the advertisement services.

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.

The Campaign Mechanics

CfA's iLAB identified a WhatsApp free internet campaign promising free mobile internet data to celebrate the 10th anniversary of the WhatsApp company. A CfA analysis revealed the process being used was to lure innocent citizens to monetised advertisement sites. We observe two scenarios when a victim is enticed by the promotion.

Scenario One

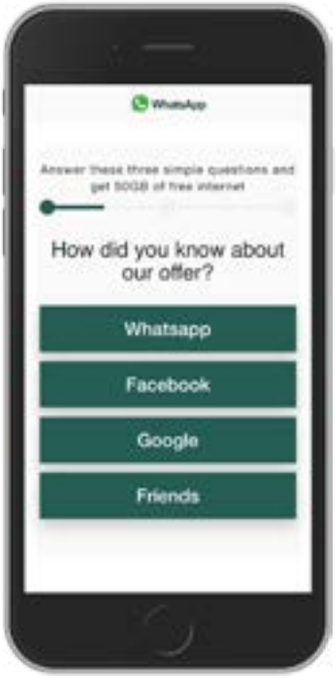
When a user clicks the shared link, they are directed to a landing page that invites the victim to answer seemingly easy survey questions.

A screengrab of the The landing page (Source: archive/CfA)

A deep dive into the source code of the website shows that the three survey questions have been hard coded into the website and any response the user selects loads the next question in the chain.

The last question redirects the victim to a page where they are required to share the campaign with 20 friends or five WhatsApp groups in order to claim their mobile data.

Survey Questions



Survey Question 1

Survey Question 1

Survey Question 1

Once the user answers the survey questions, they are prompted to share the link to at least 5 WhatsApp groups. A progress bar would keep track of the number of times a user shared it with their friends or groups

Sharing Screen

Message posted to a WhatApp group

The threshold for the number of times the victim is able to share the message is controlled by a script on the source code.

Once the victim successfully shares the campaign on WhatsApp and clicks on the 'Continue' button to claim the free mobile data, the page reloads and restarts the process.

Scenario Two

In the event that a victim visits the website but doesn't click on the ***Continue*** button as shown on the landing page, the page redirects to the url 'https://graizoah.com/afu.php?zoneid=3345594' after 6 minutes (360 seconds).

This action is controlled by the code below, extracted from the source code of the website.

```
<html lang="en-US" class="gr__rewardswp_com">
<head><meta charset="windows-1252">
<meta http-equiv="refresh" content="360;url=https://graizoah.com/afu.php?zoneid=3345594">
```

6 Minutes

According to Malwaretips.com, Graizoah.com is part of an advertising service that website publishers can use to generate revenue on their sites. Unfortunately, this is also used by malicious programs, or actors using their websites to redirect users to these Graizoah.com ads in order to generate revenue.

When Graizoah.com redirects a browser to an advertisement, the ads are typically for unwanted Chrome extensions, surveys, adult sites, online web games, fake software updates, and unwanted programs.

Some of the sites that victims were redirected to from the website under investigation range from betting sites, online ecommerce stores, virtual private network (VPN) sites offering updates, and news websites among others.

Some of these sites identified are shown below.

E-commerce Site

VPN Site

News Site

Betting Site

Betting Site

Mobile ringtones Site

The perpetrators

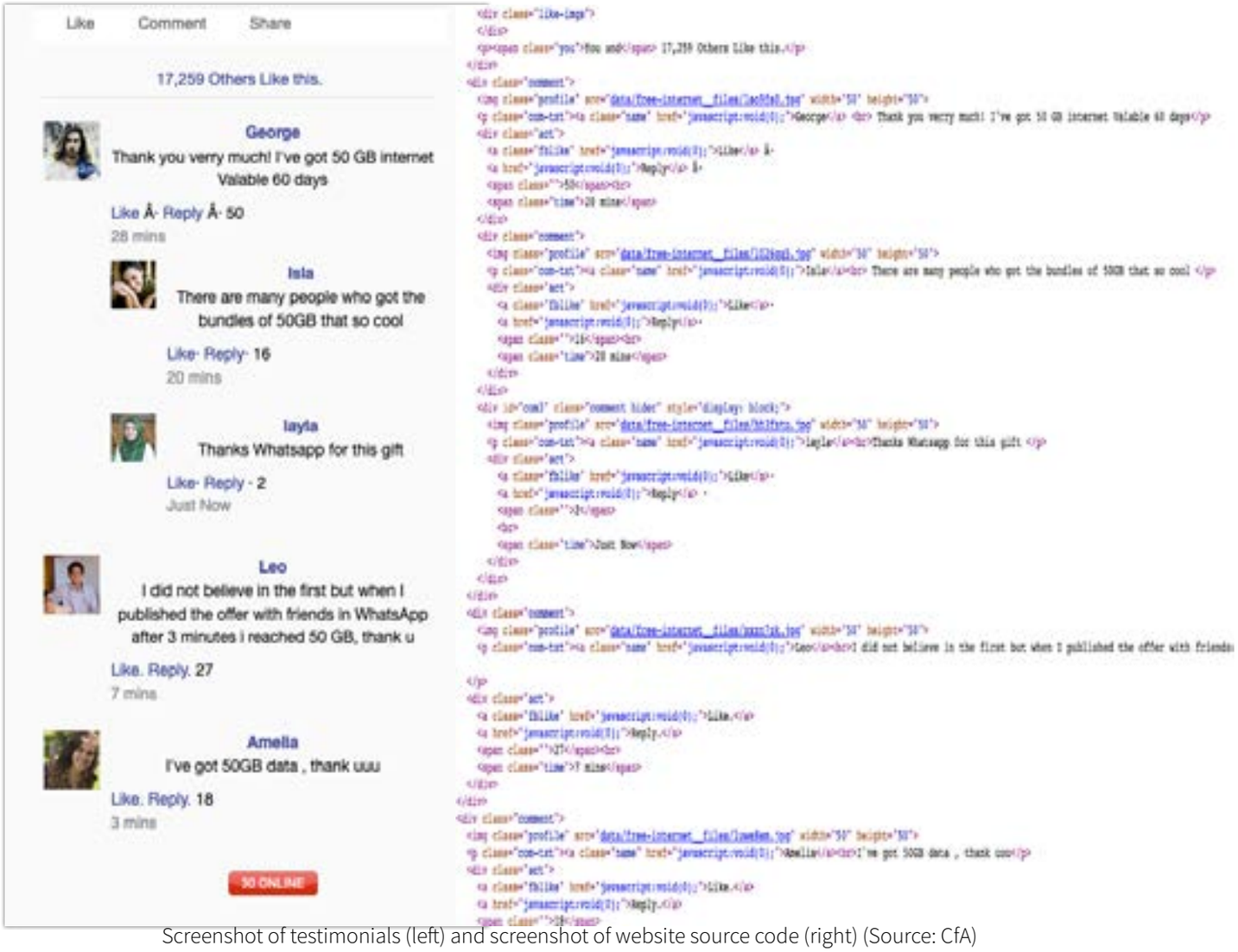
Site details

The first red-flag in the campaign is that the link provided doesn't use an official WhatsApp domain (www.whatsapp.com). Notably the subdomain has been added to create an impression of credibility.

The site also had a bright countdown sticker used to create a sense of urgency, to motivate the victims to quickly participate in the promotion. The counter sticker had a warning that there are limited offers left. This makes the victim feel that they are required to act fast.

Fake user reviews

One of the notable characteristics of the campaign website is that it had a section where users who purportedly participated in the campaign were awarded with the free internet bundle. An iLAB analysis determined that these were fake reviews/ testimonials that had been hard-coded to the website source code by the perpetrators.



Screenshot of testimonials (left) and screenshot of website source code (right) (Source: CfA)

A Google image reverse lookup for images of the profiles making the testimonials reveals that these are images lifted from the internet.

Site ownership information

A look-up to determine the ownership of the website using the Domain Name System (DNS) records revealed that the site is registered by Namecheap Inc, located in Panama. The website was created on 26 May 2020 and as at the time of the investigation, the site was 3 months and 5 days old.

The registrant organization on the Whois information for the website had however been redacted and registered to WhoisGuard Inc for privacy concerns, and therefore iLAB was unable to determine the entity or individual behind the scam.

Whois Record (last updated on 2020-09-03)

```
Domain Name: FREEINTERNETOFFER.XYZ
Registry Domain ID: D187524574-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Updated Date: 2020-07-06T09:52:31.0Z
Creation Date: 2020-05-26T10:13:27.0Z
Registry Expiry Date: 2021-05-26T23:59:59.0Z
Registrar: Namecheap
Registrar IANA ID: 1068
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
d
Registrant Organization: WhoisGuard, Inc.
Registrant State/Province: Panama
Registrant Country: PA
Registrant Email: Please query the RDDS service of the Registrar of Record identified
 in this
output for information on how to contact the Registrant, Admin, or Tech contact of th
e queried
domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in t
his
output for information on how to contact the Registrant, Admin, or Tech contact of th
```

Screenshot showing the Whois information for the domain FreeInternetOffer.xyz (Source: domaintools.com/ CfA)

Amplification

The scam used the WhatsApp chain messaging strategy to reach a mass of people, by encouraging users to share the promotion with personal WhatsApp contacts and group members, with a claim that the victims recommend the promotion and have received the award.

Website statistics

CfA noted that the promotion site uses the website www.supercounters.com, to track the statistics of the website in terms of the number of visitors and clicks.

Using the supercounters ID of the website, we noted that the website had a total of 444,529 visits (as at 1 September 2020) with an average of 4,900 daily visits from users in different countries.

The table below shows the distribution of visitor location by country.

Countries			
1.	Nigeria	197,275	43.79%
2.	Sri Lanka	71,854	15.95%
3.	European Union	40,129	8.91%
4.	South Africa	25,890	5.75%
5.	Kenya	15,182	3.37%
6.	Zimbabwe	14,941	3.32%
7.	United States	12,646	2.81%
8.	Ghana	12,565	2.79%
9.	United Kingdom	10,853	2.36%
10.	Uganda	8,185	1.82%
11.	India	6,250	1.39%
12.	Zambia	5,965	1.32%
13.	France	3,567	0.79%
14.	Germany	2,387	0.53%
15.	Cameroon	2,082	0.46%
16.	Gambia	1,898	0.42%
17.	Pakistan	1,117	0.25%
18.	Rwanda	977	0.22%
19.	Malawi	947	0.21%
20.	Saudi Arabia	893	0.20%
21.	Sierra Leone	787	0.17%
22.	Switzerland	782	0.17%
23.	Tanzania, United Republic of	741	0.16%
24.	Netherlands	689	0.15%
25.	United Arab Emirates	680	0.15%

Table showing the distribution of visitor location by country (Source: archive/ CfA)

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.

A geographic map of website's visitors from Supercounters.com (Source: archive/ CfA

The fraudsters are able to collect information on users visiting the site as shown in the screenshot taken below. The details collected for this particular site includes;

a. Location
b. Browser
c. Operating System
d. Screen resolution

Screenshot showing details of some of the visitors to the website (Source: archive/ CfA)

Old dog, New Tricks

Earlier debunks made by fact-checking organisations indicate that this is a scam that has been previously used to lure users with free internet packages. iLAB traced articles going back to 2018 as shown in the screenshot below.


BUSINESS INSIDER SOUTH AFRICA

TRENDING

No, you won't get '50 GB of Internet Data' for sending WhatsApps to your contacts

60 DAYS OF FREE INTERNET CONNECTION FAKE

GET 50 GB

- A WhatsApp message promising "50GB of free internet data in any mobile network for 60 days" keeps doing the rounds in South Africa.

Business Insider SA (2018)

On 03 December 2018, Business Insider South Africa debunked an instance of such a campaign. The scam promised 60 days of free internet connection for participants of the campaign.

In July 2019, both The Sun and Mirror in the UK published debunks on what was then a promised 1,000 GB of mobile data.


THE Sun

TRAVEL MOTORS PUZZLES SUN BINGO SUN VOUCHERS

BAD CHAT Don't click WhatsApp message offering you '1,000GB FREE internet' – it's a dangerous scam

REVEALED

1 Comment

WHATSAPP users are being warned over a new scam that offers you free internet data.

Crooks pose as WhatsApp to trick you into handing over details – and it could leave you seriously out of pocket.

WhatsApp Offers 1000GB Free Internet!

Crooks are targeting WhatsApp users with a scam text

If you receive a message from "WhatsApp" offering 1,000GB of free internet data, don't click the attached link.


Mirror

WhatsApp scam offers '1,000GB free Internet' - her are the signs it's a fake

SHARE COMMENTS

By Shivali Best

WhatsApp

Screenshots from The Sun and Mirror publishing companies showing debunks of similar scams

More scams are run by the operators using popular brands across multiple geographies, and the results are always the same. CfA identified some of them including free phones, beauty products, shoes, pizza, emoji apps and visa scams.

Samsung

L'Oreal

Addidas

Canada Visa

Dominos

Emoji Installations

Conclusion

The scam was orchestrated to target WhatsApp users, with an inauthentic campaign masquerading as a promotion from WhatsApp to award users with 50GB of data. The campaign was amplified through a WhatsApp chain messaging strategy which required users to share a link to the campaign with 20 WhatsApp contacts or five groups

With the webpage remaining active and more victims falling prey to the scam by clicking the fraudulent link, the puppet masters behind the promotion continue generating revenue from the ads..

Recomendations

We recommend that:

- Newsrooms and members of civil society should create awareness on the existence of such scams and encourage citizens to be on the lookout and report similar inauthentic activities for further investigation.
- Citizens should be trained to identify and avoid sharing/ engaging with links that purport to award users by using WhatsApp chain messaging system.

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, Niger, 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