Thellesi Trust
people matter

#FICHAUCHI CAMPAIGN

FINAL CAMPAIGN REPORT

4Th, SEPTEMBER 2023.

PART ONE: ANALYTICS FROM THE CAMPAIGN.

Item	Phase One	Phase Two	Phase Three
Duration of Campaign.	5 Weeks	5 Weeks	6 Weeks
Social Media Posts.	49	49	12
Target Audience.	Kenyans, 18-34 yrs, Mostly from rural areas.	Kenyans, 18-34 yrs, Mostly from rural areas.	Kenyans, 18-34 yrs, Mostly from rural areas.
Trending.	24hrs (Monday 12 June)	24hrs (Saturday 8th July)	N/A
Community Radios	N/A	N/A	9 community radios.
Reach.	17.4M	48.4M	49.4M *(6.1M - Social Media.* *4.4M - Community Radios* *38.9M - Citizen Tv, Tv 47, KTN News).*
Engagement	25,074	104,700	12,153

TOTAL CAMPAIGN REACH

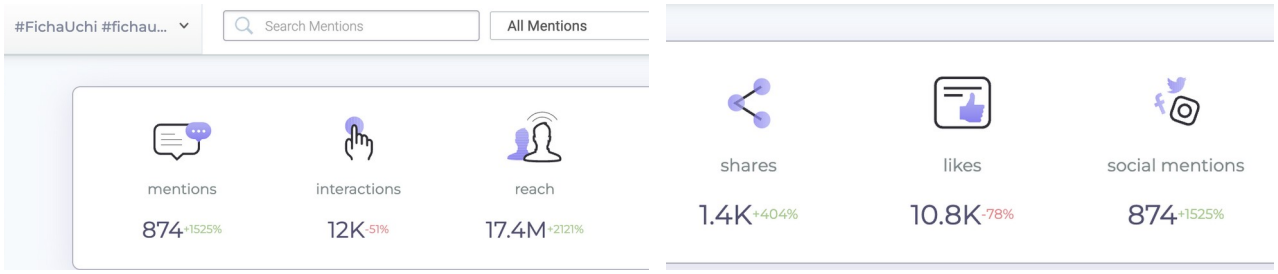
Phase.	Reach.	Engagement.
Phase One	17.4M*	25,074*
Phase Two	48.4M*	104,700*
Phase Three	49.4M*	12,153*
Total Campaign Reach	**115.2M***	**141,927***

**The numbers provided represent conservative estimates that can be tracked using social media analytics tools. The campaign reached more people via platforms like WhatsApp and those who downloaded the content and shared without using the #FichaUchi hashtag.*

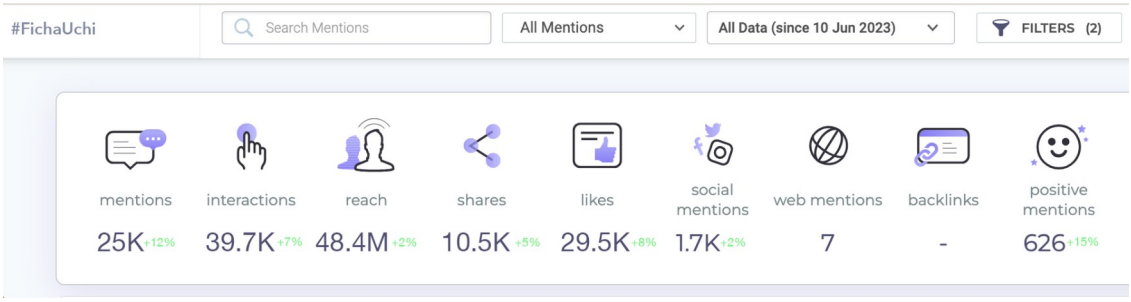
mn

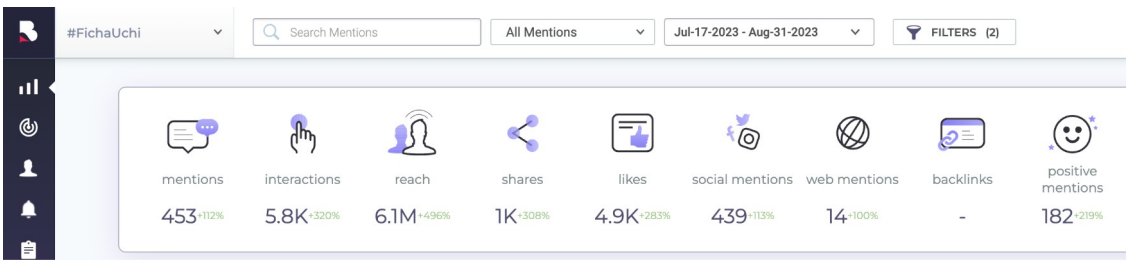
SCREENSHOTS FROM THE CAMPAIGN.

A. BRAND MENTIONS



Screenshot from Phase One (May 8th - June 9th).

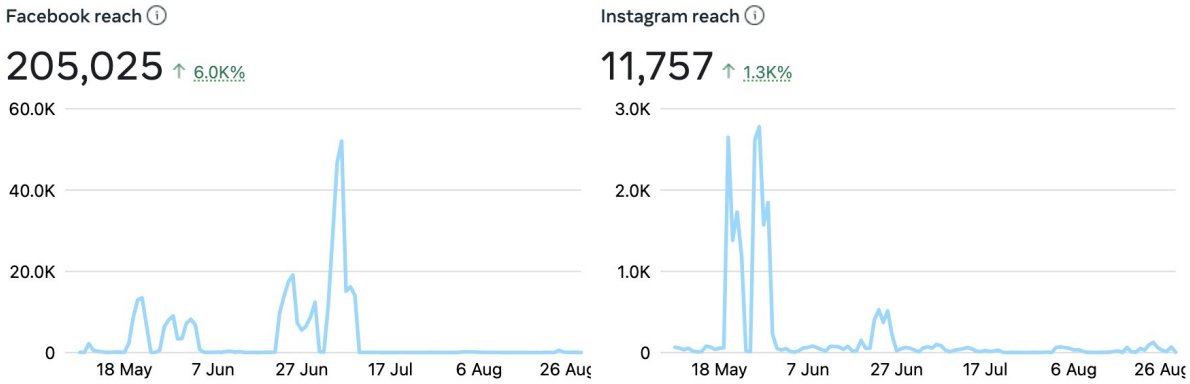


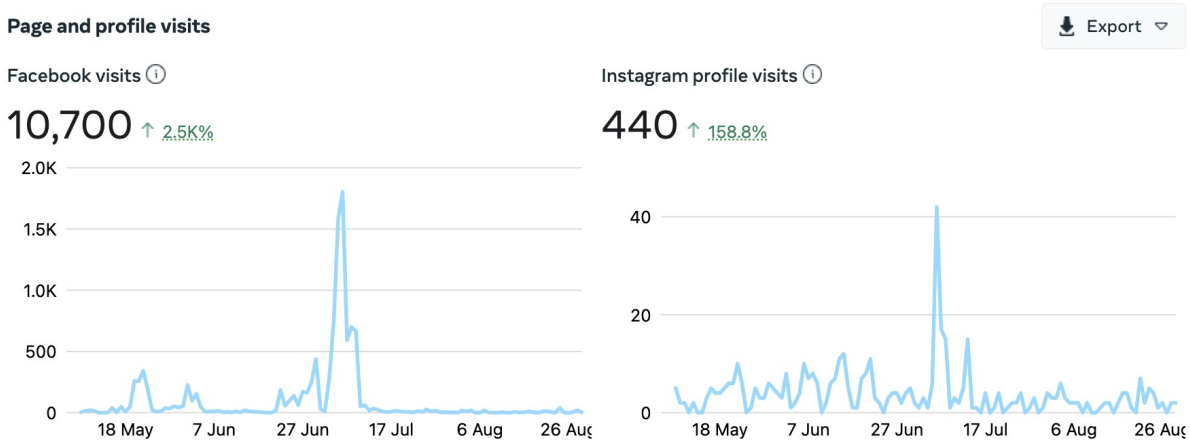


Screenshot from Phase Two (June 10th - July 17th).

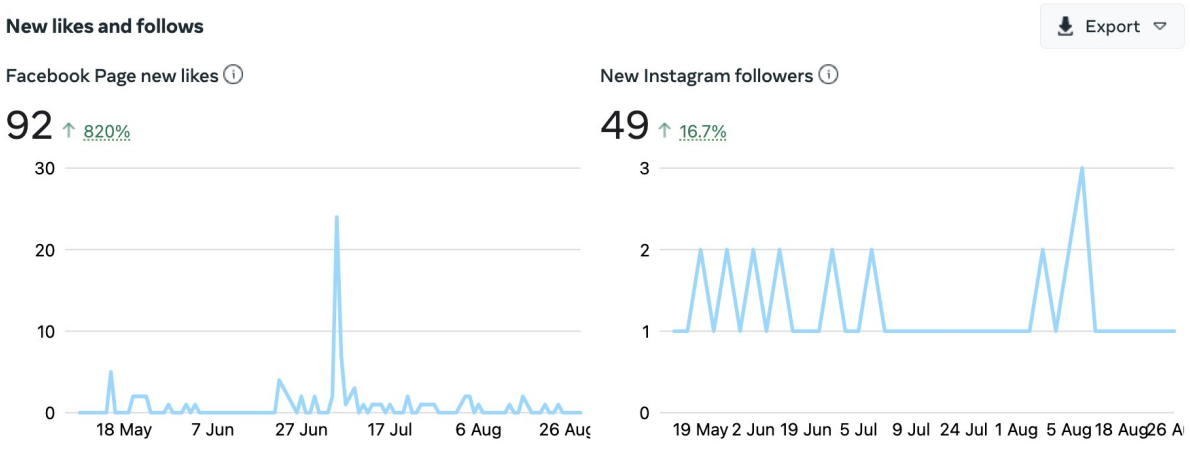
Screenshot from Phase Three (July 17 - Aug 31st).

B. FACEBOOK



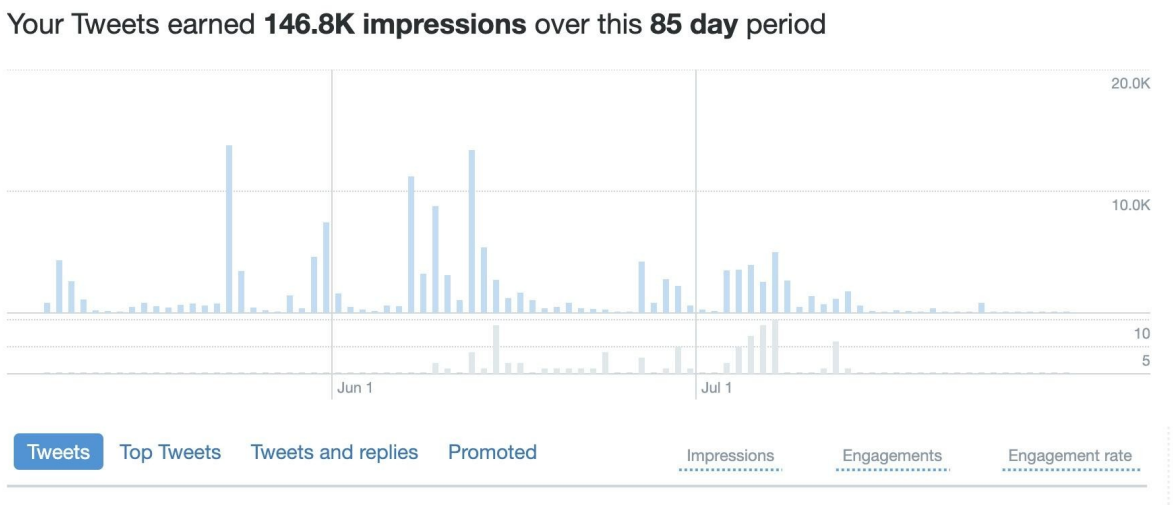


PEOPLE REACHED DIRECTLY BY THE OI META PAGES.
NUMBER OF VISITS TO OI META PAGES.

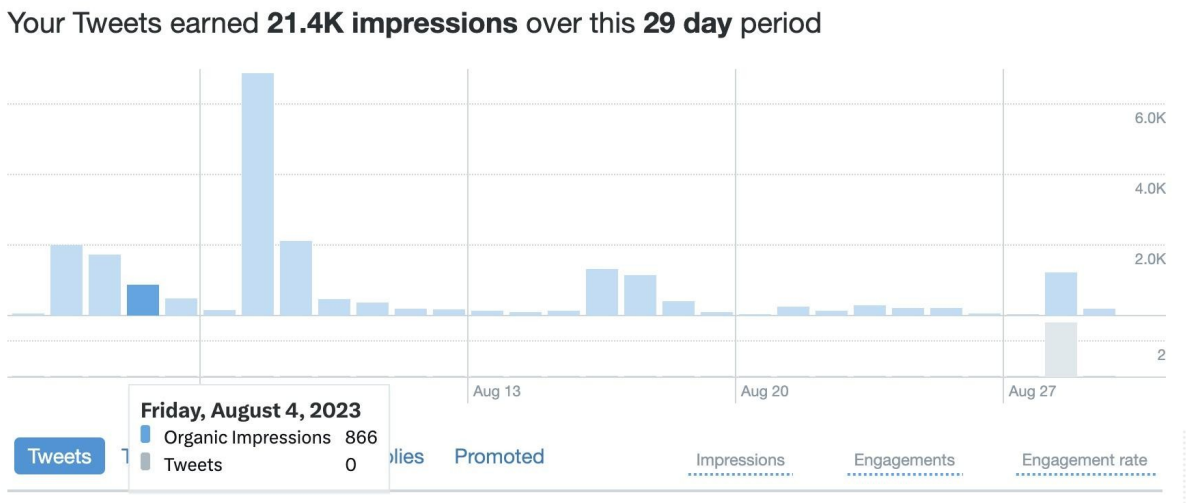


NEW PAGE LIKES AND FOLLOWS ON OI META PAGES.

C. TWITTER



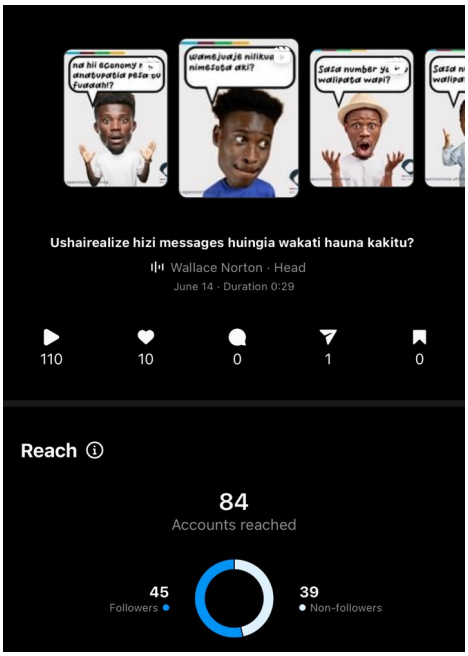
ANALYTICS FROM OI TWITTER PAGES FOR THE DURATION OF THE CAMPAIGN.

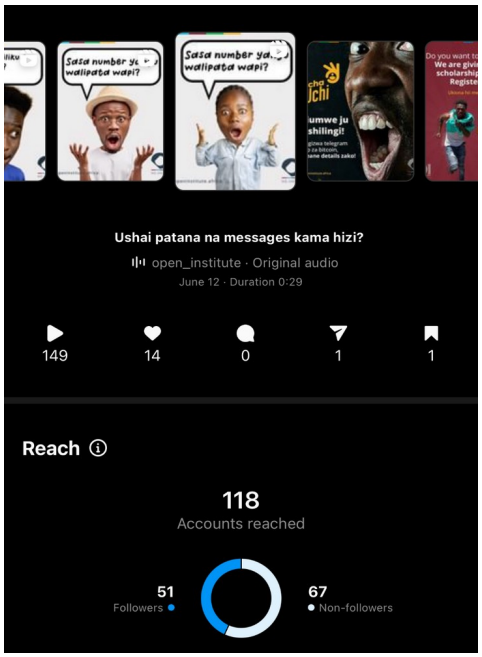


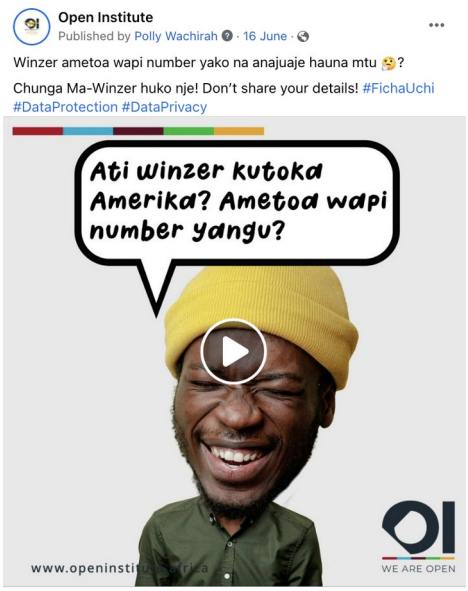
TACTICS USED TO EXECUTE THE CAMPAIGN.

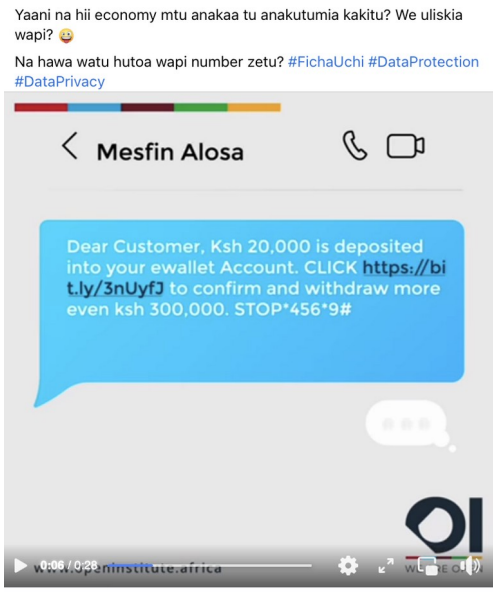
The target audience of the campaign is broad. We considered that different social media platforms prefer certain kinds of content (e.g. Facebook loves pictures and posters) and that different people within the targeted audience consume social media differently (eg 18-24 year olds consume more of tiktok than twitter). As a result, we employed different tactics to reach as many groups of people in the audience bracket as possible. Some of the things we did include creating animations, memes, short skits, partnering with social media influencers, partnering with twitter promoters, facebook boosting and sharing the posters in Facebook and WhatsApp groups.

a. **Animations** - We used animations because if done well, they are short, visually appealing and memorable. They allow you to quickly pass on a message that would otherwise not fit in a poster but also not long enough to be in a video.









b. **Memes** - In Kenya, the meme culture is high. People use memes to express themselves and pass messages. We used memes because they are easily shareable. Examples of the posters produced include the following:



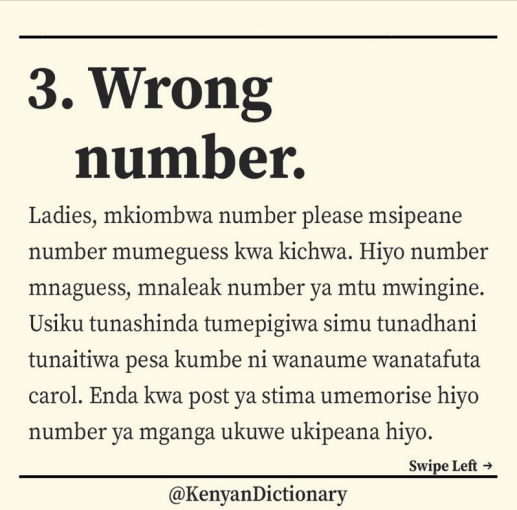


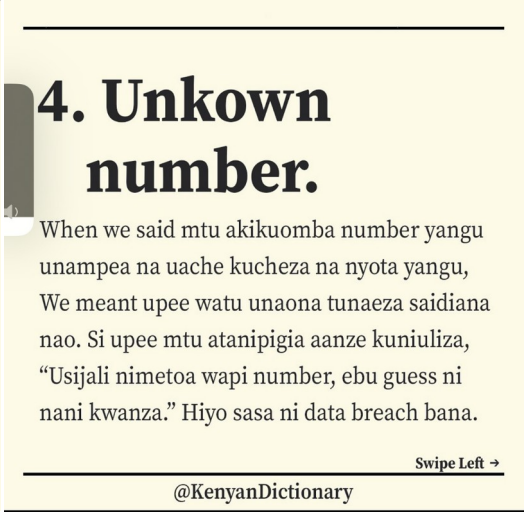
c. **Skits** - Skits are a form of storytelling that combines humour, drama and everyday life experiences to entertain an audience. We used skits to resonate with rural audiences. We used them to call attention to how we expose our personal information everyday, and explain how we can protect ourselves. We mainly posted the links on Tiktok and Instagram reels, where video content thrives. Examples of the skits produced are the following:
   - https://vm.tiktok.com/ZMj8m6KAG/
   - https://vm.tiktok.com/ZMj8mA2kQ/
   - https://vm.tiktok.com/ZMj8mrypt/

d. **Social Media Influencers** - we partnered with social media influencers to create even more visibility for the campaign. The two influencers we worked with are popular amongst the youth.

   - **J Segera -** We used Segera, a popular influencer with campus students who asks people questions on the streets. We wanted him to popularise the phrase #FichaUchi and to get campus students to share experiences of when their data was exposed. See his videos https://vm.tiktok.com/ZMj8mMTyT/ and https://www.instagram.com/reel/CtbTofWgjda/?igshid=MzRlODBiNWFlZA==

- **Kenyan Dictionary** - The Kenyan Dictionary is an instagram page that defines popular Kenyan phrases and gives examples of how they are used. We worked with them because they create very relatable content and have good engagement on their posts. We wanted them to popularise #FichaUchi as a call to action for Kenyans to protect their personal information. Here is their video - https://www.instagram.com/p/CuWvw68sqSo/?

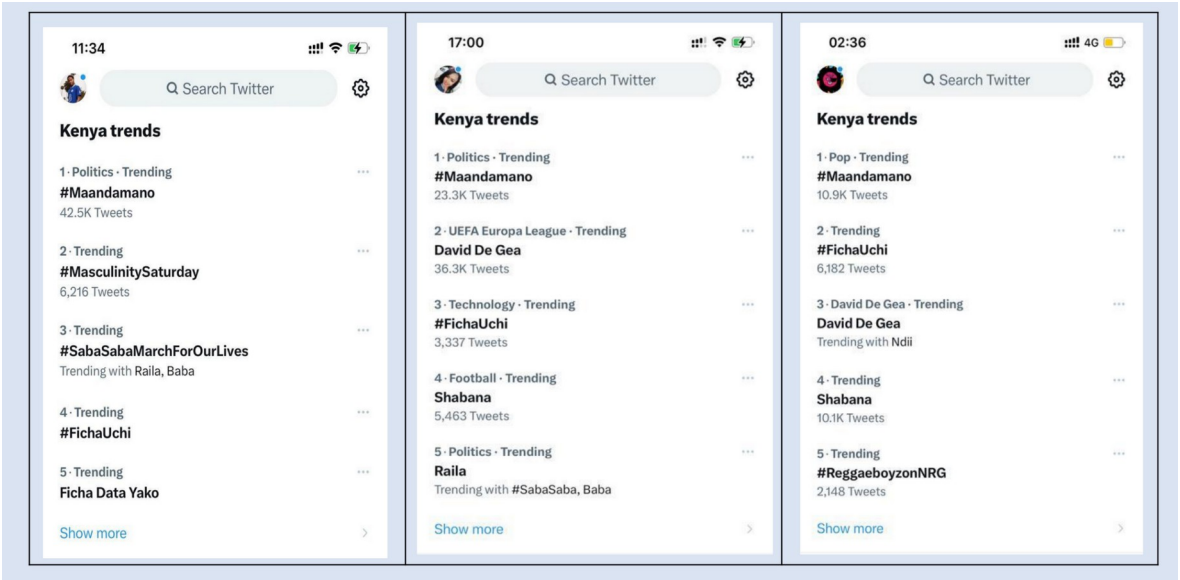




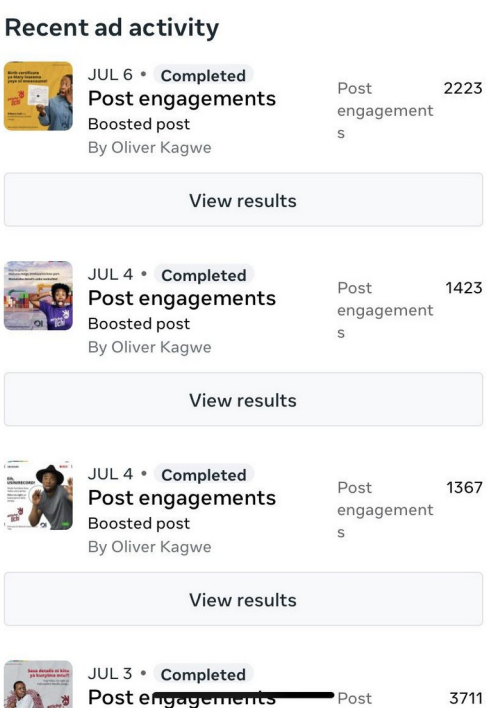
igshid=MzRlODBiNWFlZA==

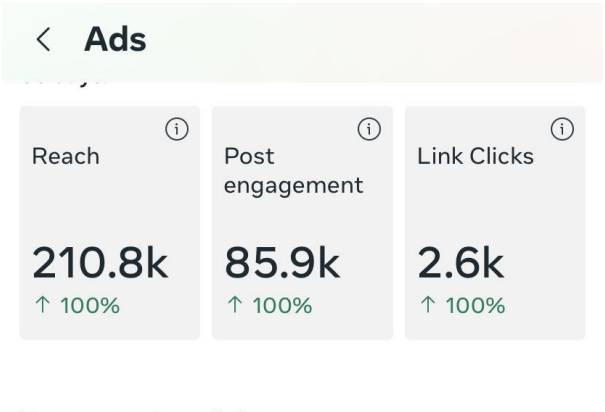
e. Twitter Promoters.

Through twitter influencers, we got #FichaUchi to trend on Twitter.



f. Media buying.





g. Twitter Influencers - We worked with Janet Machuka, Barack Otieno and Africa Tweet Chat to push the content. With their huge following and heavy social media presence, they contributed to increasing the reach and engagement of the campaign.

PART TWO: FOCUS GROUP DISCUSSIONS & RADIO TALK SHOWS.

THE GOAL OF THE FOCUS GROUP DISCUSSIONS (FGDs):

1. Understanding on what the participants know/don't know about data, data protection and related concepts.
2. Understanding how and why the participants use, share and protect their personal data.
3. Getting the participants' perceptions of data privacy and data protection.
4. Understanding where participants get information about data privacy and protection and how this shapes their behaviours.
5. Identifying what type of information or education the participants feel is necessary to enhance their understanding of data and data protection.

Linked **here** is the brief we used for the FGDs. We used it as a guide in the actual sessions to make sure that we covered all the questions.

DETAILS OF THE FOCUS GROUP DISCUSSIONS.

Location	No. of Participants
Nairobi	18 *(11F, 7M)*
Nakuru	16 *(8F, 8M)*
Kisumu	16 *(9F, 7M)*
Kilifi	16 *(8F,8M)*
Mombasa	14 *(7F, 7M)*
Machakos	15 *(7F, 8M)*
Embu	16 *(11F, 5M)*
Kakamega	16 (*9F, 7M)*
Siaya	17 *(11F, 6M)*

KEY FINDINGS FROM THE FOCUS GROUP DISCUSSIONS:

The following are some of the main findings from the Focus Group Discussions:

1. All the participants have been called, texted, inboxed or emailed by strangers, advertisers, recruiters and others. The most common scams across the counties include:

- Scammers posing as teachers and asking parents to send them money for their children's school requirements such as calculators or hospital bills.
- Scammers using one's profile picture on WhatsApp to solicit money from one's contacts.
- Scammers hacking one's Facebook accounts and using the accounts to solicit money from their friends and families.
- Recruiters offer fake jobs and ask for registration/booking fees on platforms like Facebook and WhatsApp.
- Tricking people into clicking links that lead to websites that collect information such as name, phone numbers, email addresses. They also have cookies that collect and store even more information.
- Getting a fake message about money sent to their Mpesa account, followed by a call asking for the money back.
- Getting a call by a lady who claims to have containers full of supplies stuck at the port. She then requests one to send her a certain sum of money for her to get the container released, upon when she shall return the money or share a percentage of the supplies in the container.
- Being called by scammers alleging to be customer care agents of mobile service providers or banks. They ask a few questions and give a set of instructions to the unsuspecting user, upon when they manage to take over or swap one's phone number.

Many of the participants didn't report these scams because they were embarrassed or didn't think they'd get help from the police if they reported.

There are those who reported the scams, but many of them did not find any help at the end of their efforts.

2. The most common examples of personal details known by participants include phone numbers, IDs, birthdates, account numbers, Pin numbers and passwords. But very few participants mentioned sensitive data like tribe, where they live or their medical history.
3. Many participants felt that they are arm twisted to share their personal information in exchange for services. "We don't have much of a choice to opt out of sharing our data. It's either you give them what they are asking for or you don't get to use their service/product." They expressed that this made them feel vulnerable, powerless and sometimes, exploited.

4. The participants expressed that they had very little trust placed on the police to assist a victim of scamming. They said it is easier to accept and move on rather than report to a police station. Instead, people trust social media more to take action against an organisation/person that has been found to misuse people's data. You can get 'cancelled' online and it will hurt your business.
5. Participants would rather not sue big companies for misusing their data because not only can you not afford a lawyer, but you also risk getting killed.
6. Participants expressed that they do not know what happens to their data after they have shared it.
7. They told us that joblessness or underpayment increases their chances of being scammed. The poorer and desperate you are, the more you will be scammed. This means that they are more likely to fall into a scam if it has the promise of money or a job.
8. The group also said that, "we all know when we are being scammed." Except that they fall into scammers traps again and again because each time, they hope that something good will come out of it. This happens mostly in those scams that have the promise of a reward at the end.
9. None of the participants knew what cookies are or what they do. However, some know that you get kicked out of some websites if you do not accept cookies.
10. People don't read terms and conditions because they're long, complicated and written in small fonts. They also don't read because they are usually in a hurry to use the service.
11. The data mostly collected is ID numbers, phone numbers, marital status, emails and names.
12. When asked why their data is collected, the participants explain that it is for security or reference reasons. Asked who told them, they said they "think" and "it is obvious".
13. Most of the participants said they don't know why their data is collected. No one explains to them why it is being collected, where it will be stored and who else has access to it..
14. Participants said that if those collecting data explained why they needed it, how they kept it safe, and promised to delete it in case they didn't need it anymore, they would trust them more.
15. Generally, participants would like to be told why their data is being collected, how it will be stored, and who has access to it.
16. Participants expressed a range of actions they would take in response to a data breach, including changing passwords and monitoring accounts. However, none of them mentioned reporting to authorities.

17. While some participants knew their rights as data subjects, they were not clear whether these rights are in the constitution. Some even thought that even if these rights exist, they might not make a difference because they lack trust in the country's justice system.
18. While most participants didn't think personalised ads were a good idea, some thought that this made their work easier and it gave them a variety of items to choose from. Even so, they would not be comfortable sharing more data to improve their personalised services.
19. Many participants expressed a need for more accessible and comprehensive education on data rights.
20. About half of the participants had come across #FichaUchi campaign online.
21. Many participants were familiar with terms such as privacy, data, personal data, data protection, and data rights. Definitions varied, and they were not necessarily accurate but participants generally understood their broad implications.
22. Very few participants were familiar with terms like Data Protection Commissioner, Data Controller, Data Processor, and Data Subject, although their definitions were not always accurate, the few who were familiar with the terms had only heard about them but didn't know what they meant. Those who knew had worked for CSOs at some point in their careers.
23. They also suggested that the government should partner with youths and other organisations to create more awareness about data protection. Additionally, they suggested that data protection should be taught in schools so as to create a culture of safeguarding one's personal data from a young age.

RADIO TALK SHOWS

In an effort to promote awareness and understanding of data rights among local communities, we did talk shows across nine community radios in nine counties. The primary objective of the talk shows was to engage listeners in discussions related to data protection, educate them about their rights as data subjects, address common data-related challenges faced by Kenyans, and create awareness around the office of the Data protection Commissioner as one of the solutions to tackle data related issues effectively.

Here is the brief we shared with the radio stations.

Radio	**County**	**Estimated Reach**
Ruben FM	Nairobi	380,000
Mtaani Radio	Nairobi	450,000
Radio Mikayi	Siaya	550,000
Jowi Radio	Kisumu	400,000
Radio Yetu	Nakuru	600,000
Radio Isikuti	Kakamega	300,000
Kimuri FM	Embu	550,000
Sheki FM	Mombasa	400,000
Lulu FM	Kilifi County	750,000

PART THREE: **OUR OBSERVATIONS.**

Having run the campaign for about 4 months, here are the observations that we have made:

a. More people in cities and towns can define the word data in the context of information. We attribute this to the increased conversations about data in the last couple of years. However, rural communities may not be able to easily define the term data as they are faced by challenges such as illiteracy, lower social media consumption and lower exposure to the world's trends.

b. The conversation of data protection is personal. Generally, people do not walk around thinking about their personal data, until they have been scammed and suffered loss.

c. The general feeling is that whether or not one knows their data rights, one cannot do anything about it lest they are denied access to the platforms, services or products that they need.

d. People are not aware of the Data Protection Act that protects them from having their data misused. Additionally, they are not aware of the Office of the Data protection Commissioner, her mandate and how she can “help me when my data has been breached.”

e. The community radio engagement that we did was a great way of taking the conversation directly to the communities. It allowed us to expound on the complex topic and to engage listeners who had questions.

f. We acknowledge that we did the campaign during the first year of the new government, which has been topping the headlines. Since August, online conversations have predominantly been about politics and the economy, which are highly relevant and pressing topics. As a result, our campaign occasionally got lost in the conversations, or was not aligned with people’s emotions.

g. We observe that during the World Coin scandal, a lot more conversations about data privacy were happening, from multiple sources ie, media, Civil Society, Companies and Citizens. In the 2 weeks that this scandal was happening, a lot more people knew about their data rights and the ODPC than before.

h. We think that Facebook reduces the amount of people a campaign reaches to nudge one into boosting. Once you boost, it also reduces the reach and prompts you to “reach more people” by spending more money.

PART FOUR: OUR RECOMMENDATIONS.

Going forward, we recommend the following:

1. **Behaviour change takes time. There is a need to reinforce the messages and ensure that they remain ingrained in people's habits and decision making processes.**
    - More social media campaigns.
    - More mainstream media campaigns.
    - More community radio engagement.

    As the world continues to figure out how to navigate the ever changing digital world, data protection and privacy remains a concern. Campaigns help to build a more aware and informed citizenry.

2. **Create a lovemark for data protection in Kenya. We imagine this as a social media page on its own, or a website, carrying all the content that the Open Institute has under #FichaUchi.**
    - A knowledge hub for everything data, data privacy and data protection in Kenya.
    - A place where people ask questions relating to data protection.
    - An authority that plays a watchdog/whistleblower role for the benefit of Kenyans.

    This will also help to concentrate all content in one place and not have to scroll through other Open Institute's posts to find the ones talking about data privacy and protection.

3. **Take data protection to the ground.**
    - More community radio engagement, as they are closer to people and they understand the nuances of their communities.
    - The use of Out-of-Home advertising such as billboards, to get more eyes on the campaign, arouse curiosity and encourage conversations.
    - Create champions (influencers) of data protection in different counties who help push the hashtag in their areas. These could even be Community Based Organisations.

4. **Partnerships.**
    - When the World Coin story happened, everyone came together to talk about data privacy and protection. We suggest the creation of a consortium of sorts that keeps this conversation going even when there is no scandal.

5. **Lastly, and tied to all the above, a lot more investment needs to go into running Social Media campaigns. Kenya's population is young, with many of them having access to a smartphone. Just like the private sector is leveraging the power of social media to influence consumer behaviour, the nonprofit sector should borrow from them and leverage social media to influence positive behaviour in the society. Increased investments will allow for, among other things:**

- Organisations to get the right talents to create better campaigns eg, consulting an advertising agency.
- Access to better tools to track and monitor the impact of the campaign even beyond analytics.
- More partnerships with established social media influencers and content creators who play an integral role in inspiring new behaviours.
- More paid advertising on different social media platforms.