

# ⚠️ NEW PHISHING SCAM ALERT ⚠️

**Digital marketers and social media managers** are particularly prone to cyber attacks such as phishing, ransomware attacks and spoofing!

This is a case study of an attempted phishing attack, to gain access to **MY Facebook account**.





# CONTEXT

Digital marketers are responsible for the digital presence of organisations.

They typically have access to important company assets such as websites, social media pages, google profiles etc.

In this case, access to a Facebook page, guarantees access to a business page, that has access to ad accounts that have access to bank cards that may be pre-loaded with thousands if not hundreds of thousands of dollars of company ad spends.

Secondly, social media pages are a valuable asset to organisations. Attackers might hold access to these pages as ransom and demand a certain fee to regain access.

Yes, this happens, and people have paid lots of money to get their pages back.



# SO WHY WOULD ATTACKERS TARGET SOCIAL MEDIA MANAGERS/DIGITAL MARKETERS FOR PHISHING?

## **Access to High-Value Ad Accounts**

Digital marketers often handle ad accounts with substantial budgets, thousands of dollars if not hundreds of thousands of dollars. Gaining access to these accounts allows attackers to misappropriate funds for fraudulent campaigns or personal gains.

## **Control Over Multiple Business Pages**

With admin privileges on client accounts, attackers can hijack business pages, spread misinformation, or scam followers.

## **Personal and Professional Data**

Phishing attackers can harvest sensitive client information, including contact details, business strategies, and insights, to exploit for malicious purposes.

## **Gateway to Other Platforms**

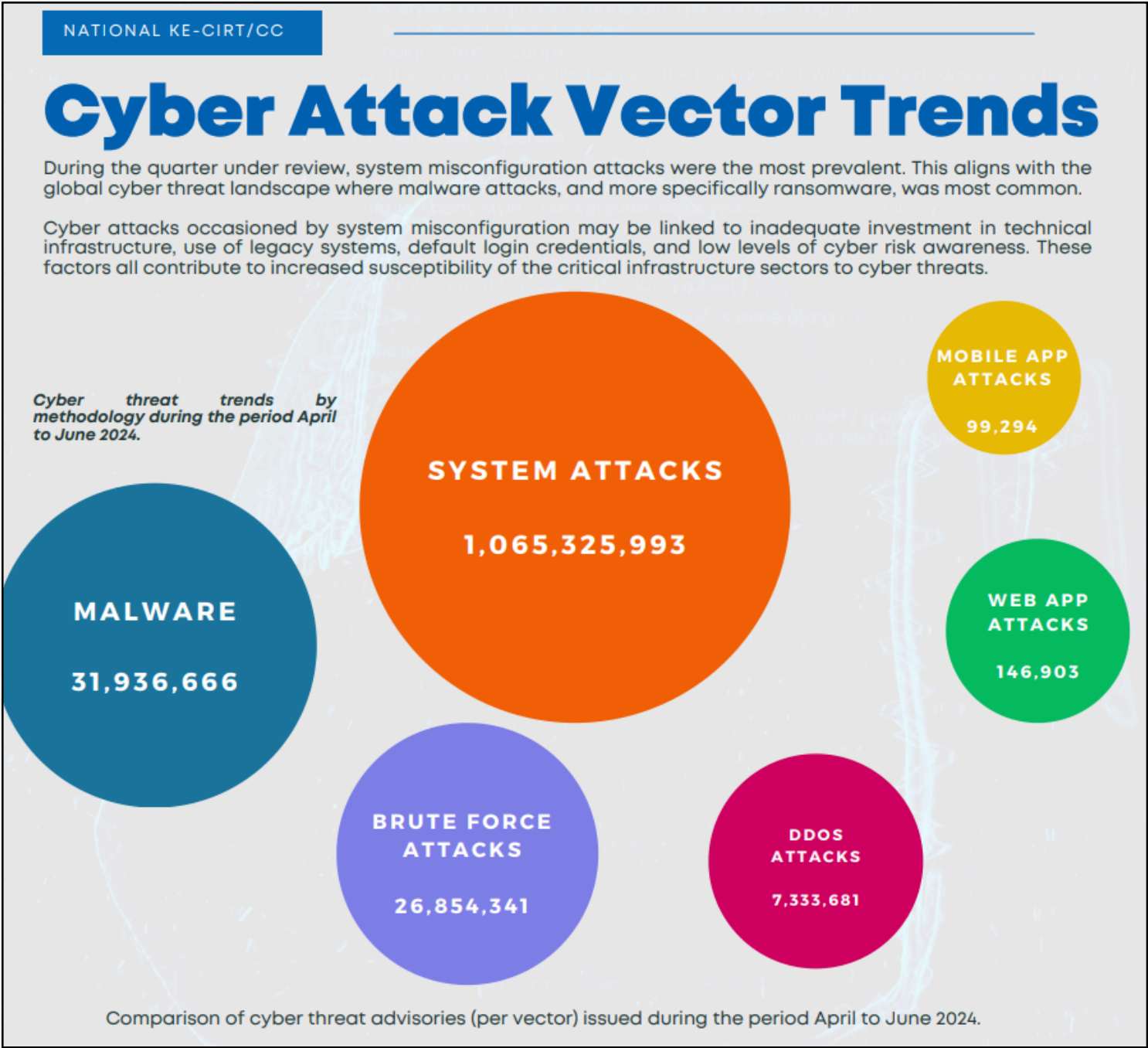
Many managers have linked accounts (like Instagram and WhatsApp), making a Facebook breach a stepping stone to other platforms.

## **Reputation Damage**

Compromising a manager's account can lead to posts or ads that harm the brand's image, eroding trust with clients and their audiences.



# Malware, specifically ransomware was the second highest form of cyber attack in the country



Cybersecurity Report A  
report by  
Communications  
Authority of Kenya.  
April - June 2024



## THE THREAT IS REAL

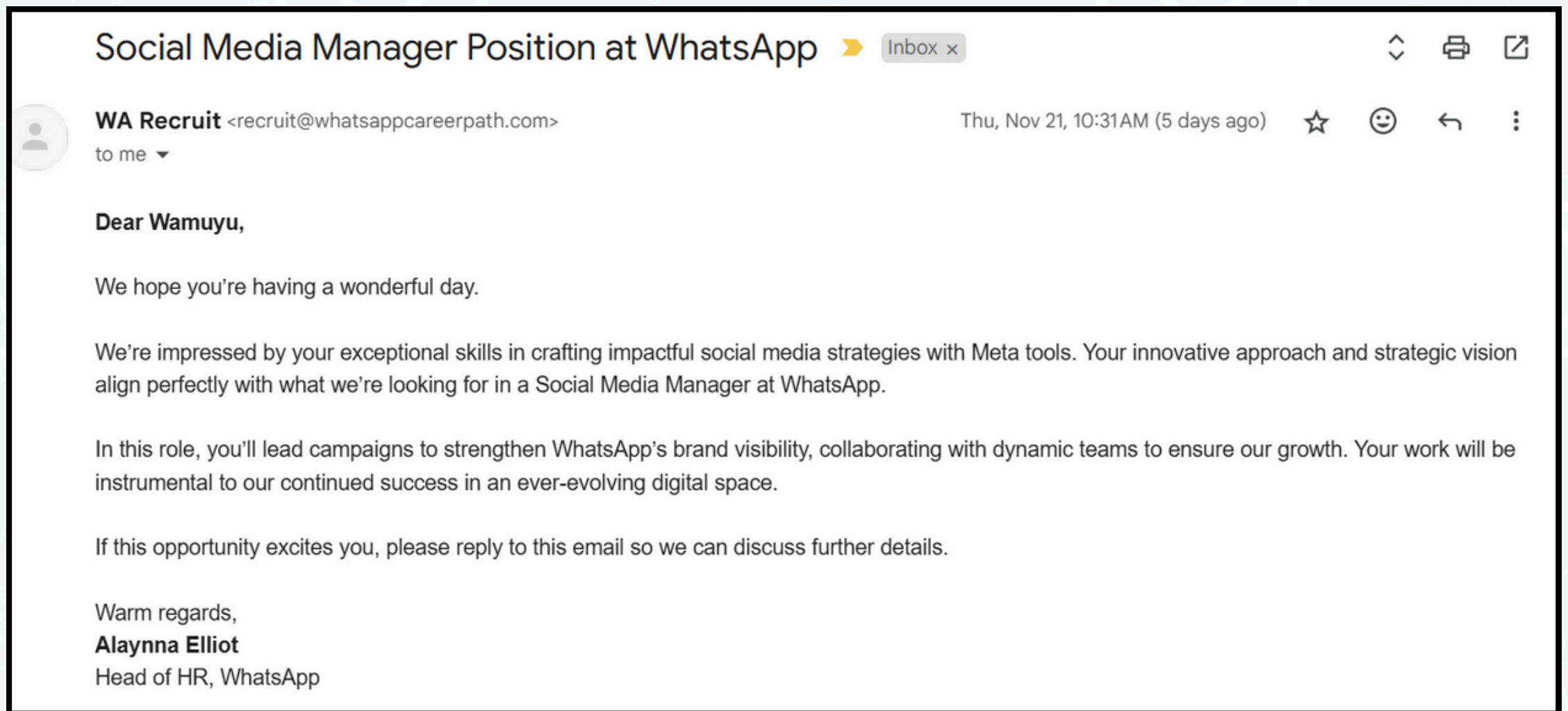
As digital marketing and communications professional, I have experienced countless phishing attempts over the years, but not as many as I have in the **last two years!**

These people are getting smarter and smarter by the day! I thought to write about it, so that we all stay vigilant.

So, how did this particular attempt start?



# IT STARTED WITH AN EMAIL FOR A JOB AT WHATSAPP





Very inviting! I mean, which digital marketer wouldn't want to work for the the worlds largest social media company?

PS: I hadn't applied for such a role, but I have previously been interested in a role at Facebook. I first thought, maybe they share candidates data cause it's basically the same company! On further look though.... I noticed some RED FLAGS!



# Quick background check




**Alaynna Elliot**  · 3rd


Director, Head of HR at WhatsApp

Los Gatos, California, United States · [Contact info](#)

500+ connections

[Message](#) [Pending](#) [More](#)

[WhatsApp](#)

[Monash University](#)

I looked up the name on the email signature, the profile checked out. But why is the director of such an organisation doing recruitment?

**WA Recruit** <recruit@whatsappcareerpath.com>  
to me ▾

The URL on this email was DEAD!  
WHY??


About this profile

**Alaynna Elliot**

**Joined**  
November 2009

**Contact information**  
Updated over 1 year ago

**Profile photo**  
Updated over 1 year ago

**Verifications** 

**Workplace**  
WhatsApp: Verified using work email  
Less than 6 months ago

[Learn how members verify information](#)

# I responded to them with my concerns



**Wamuyu Wachira**

to WA ▼

Hey, I appreciate your reaching out.

I question the legitimacy of this email though, there are a couple of red flags I've noticed.

Starting with, how's is it that the global head of HR is the one recruiting?  
Secondly, the domain from which you're email address is attached doesn't exist.

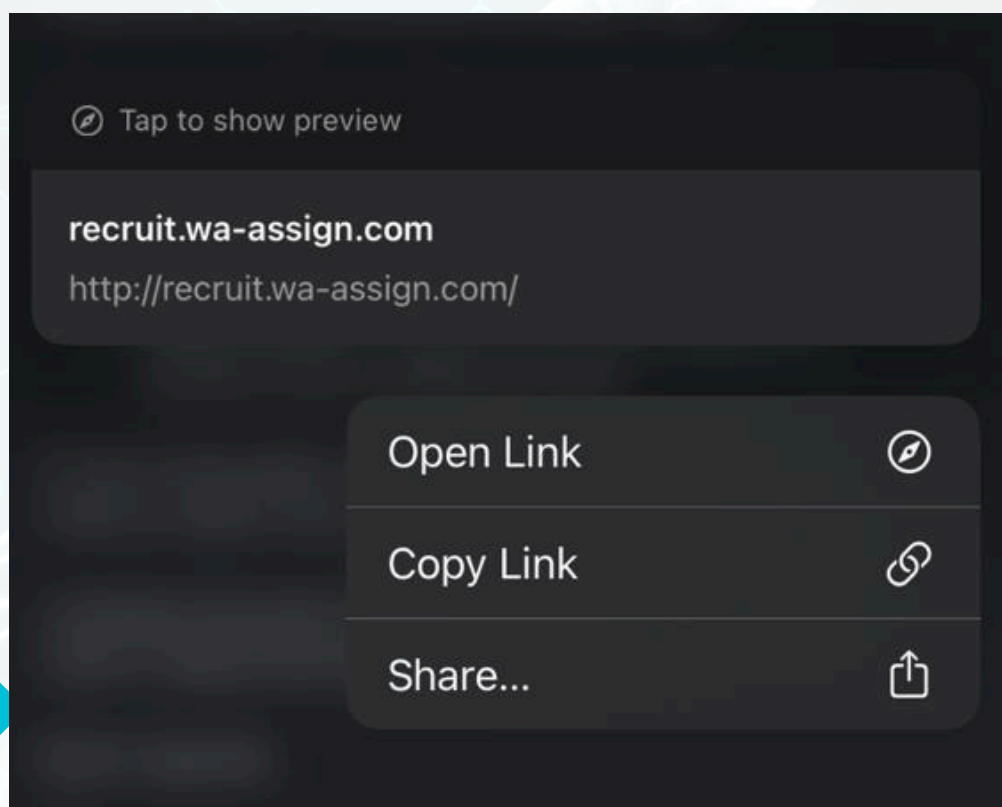
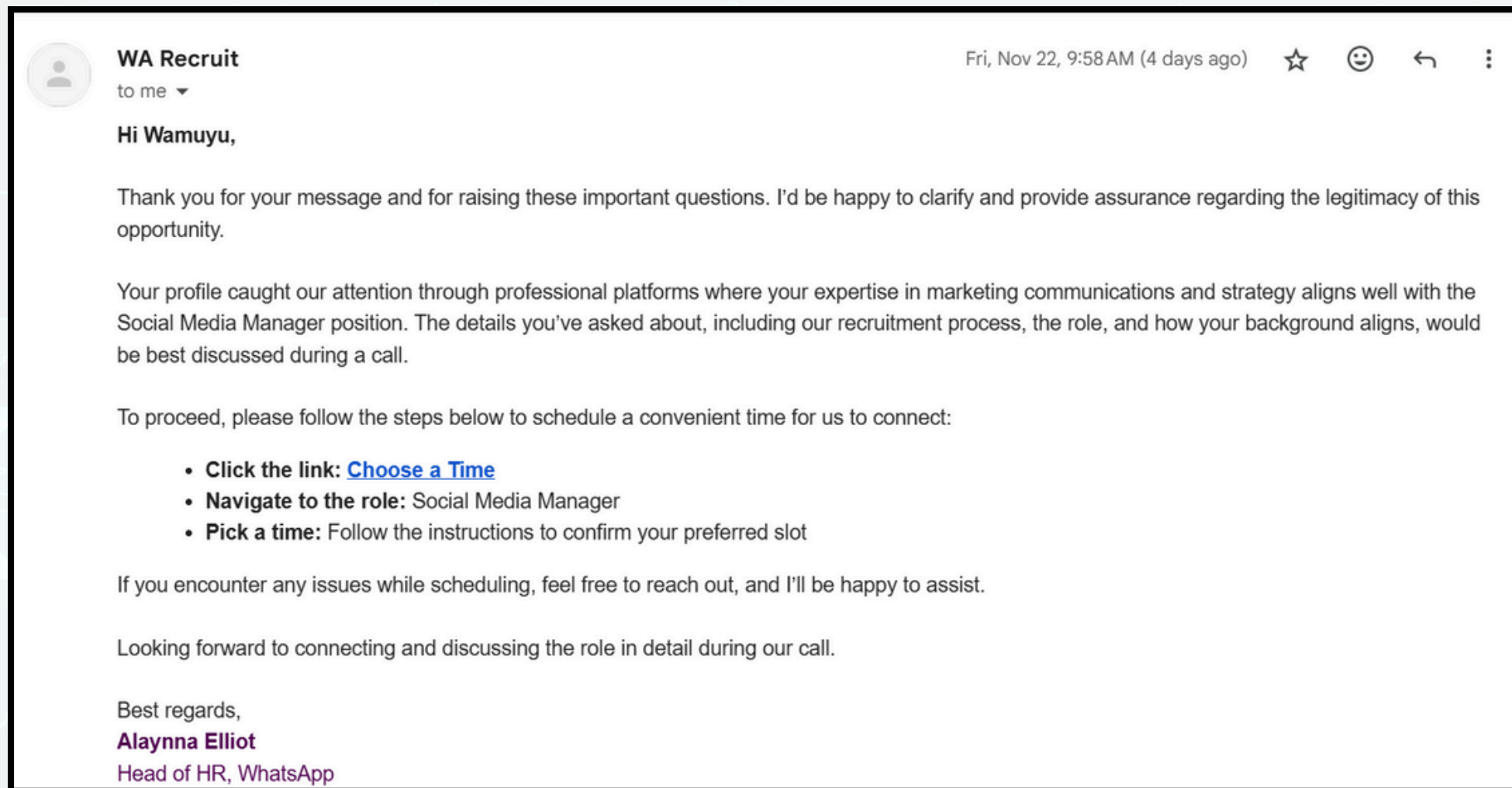
Why is it not a .meta domain name?

Lastly, where do you get my details from?

Please clarify the above, thanks.



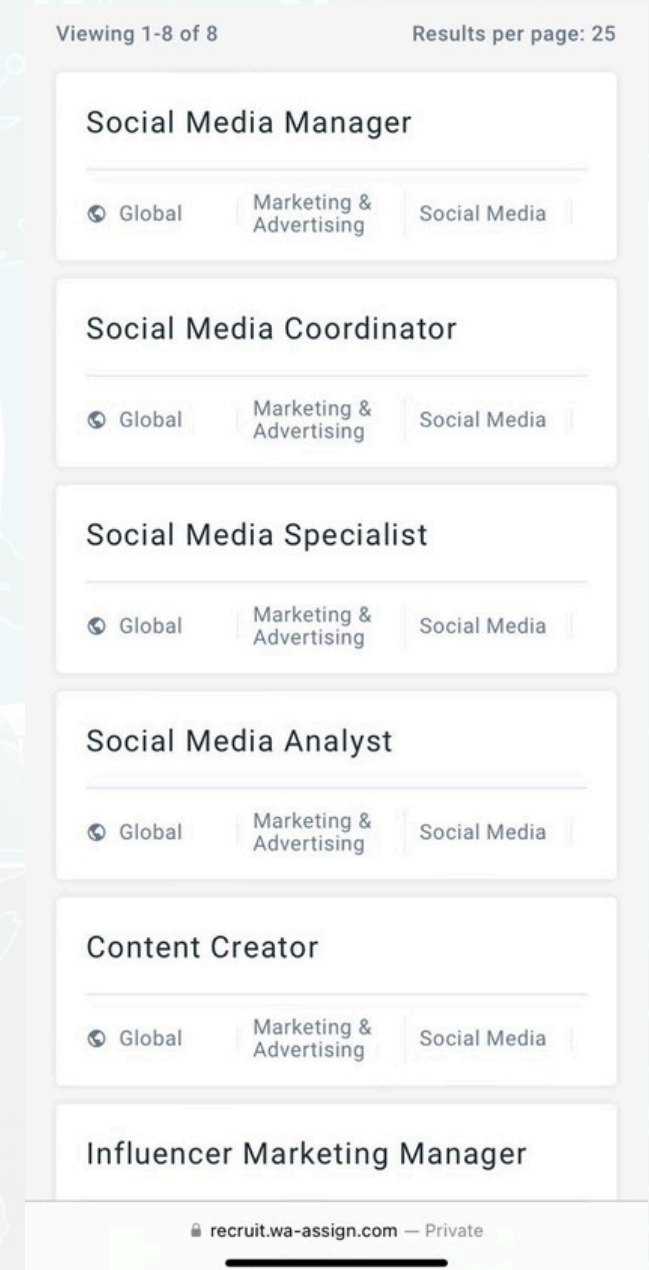
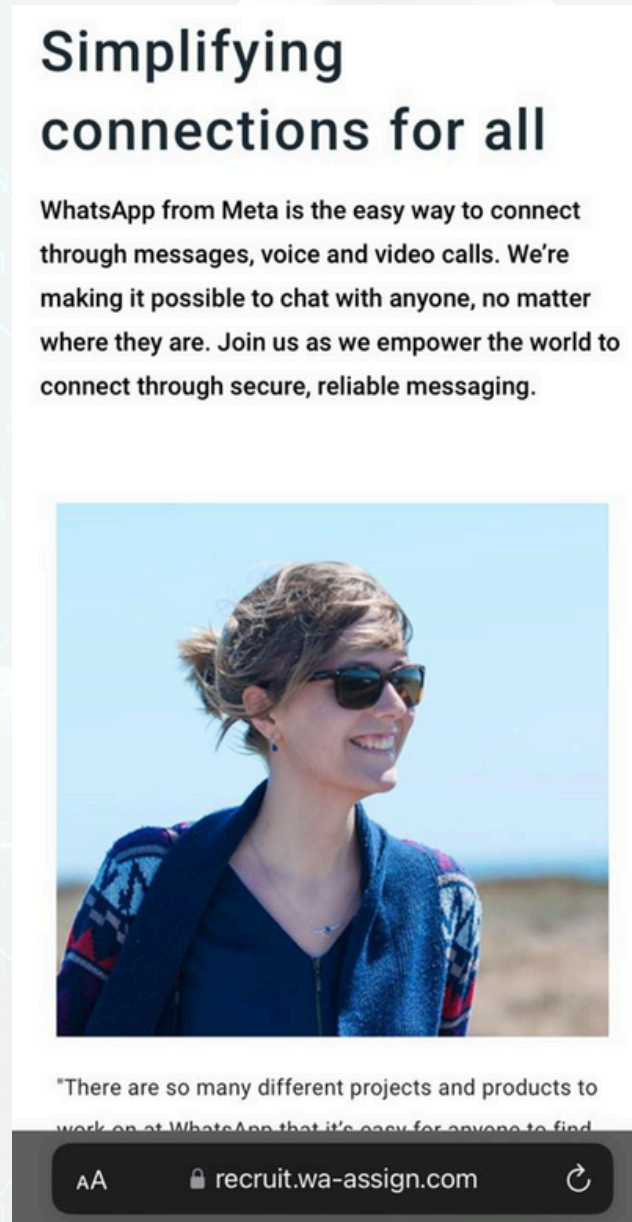
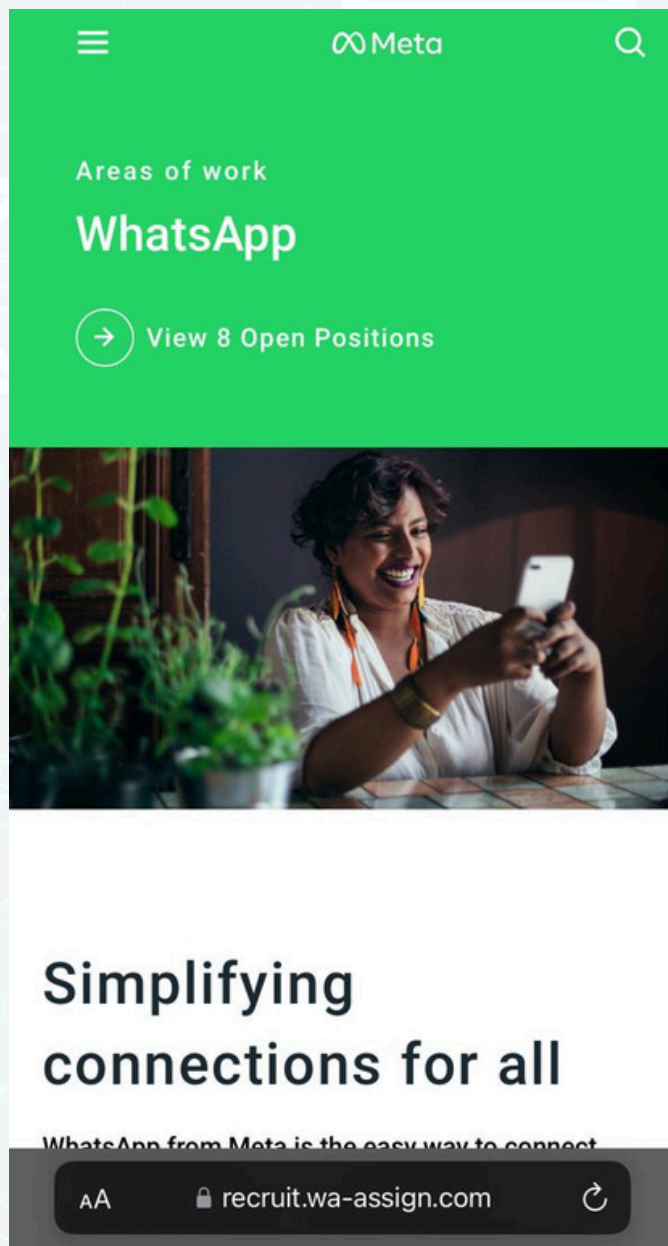
# They got back to me



Sounds professional, you know!  
They asked for a call, almost  
sounds legit! But was it?

On inspecting the hyperlink,  
this is what the url looked like.

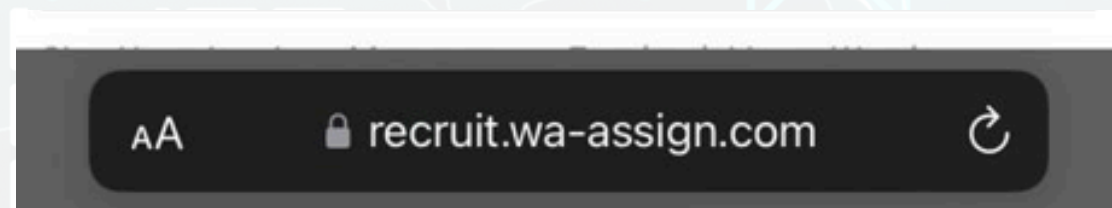
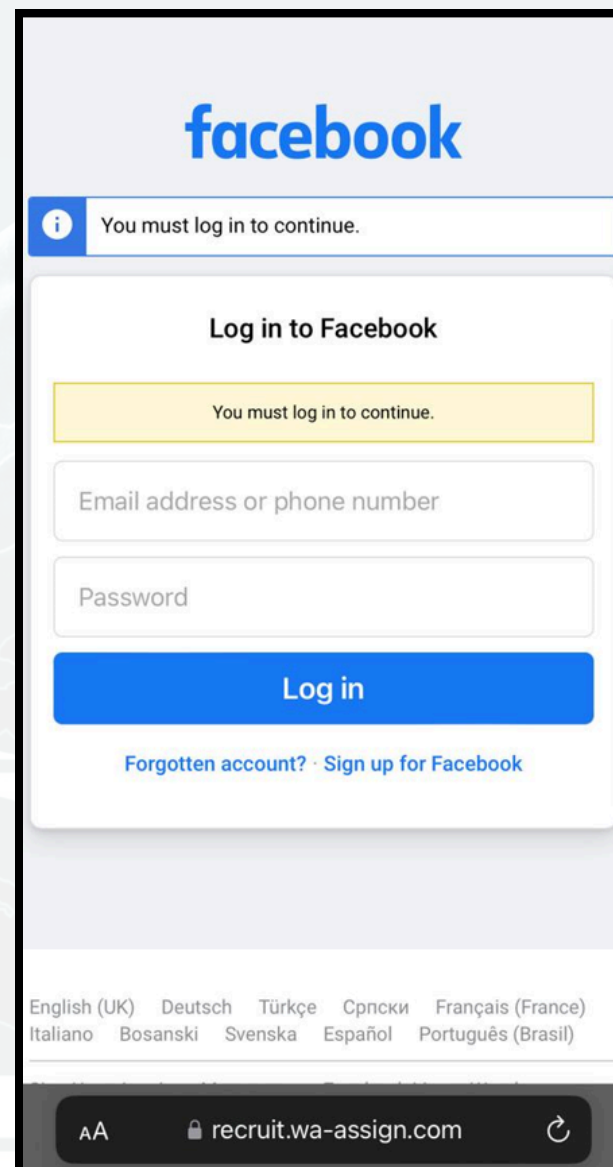
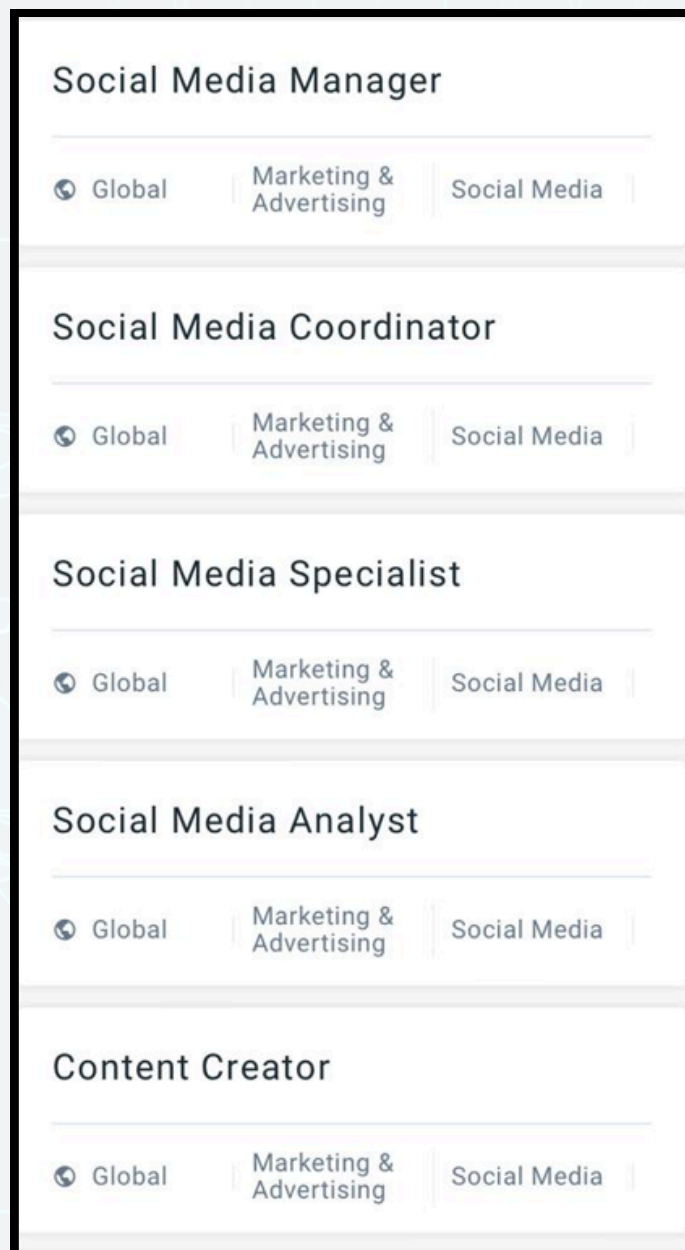
# I clicked on the link. Please don't do it if it happens to you!



The landing page looked very Whataspp'y with the brand colours, brand comms! Easy to navigate, they did well with the page tbh! Very convincing!



# Where they get you!



The role directly sends you to this landing page that requires you to log in to your facebook! Once you input your details, they capture your email and password and that is how your page disappears!!

# I needed to get to the end of this, but they ghosted me!

Wamuyu Wachira <

to WA ▼

Thanks. I prefer we use my meeting link.

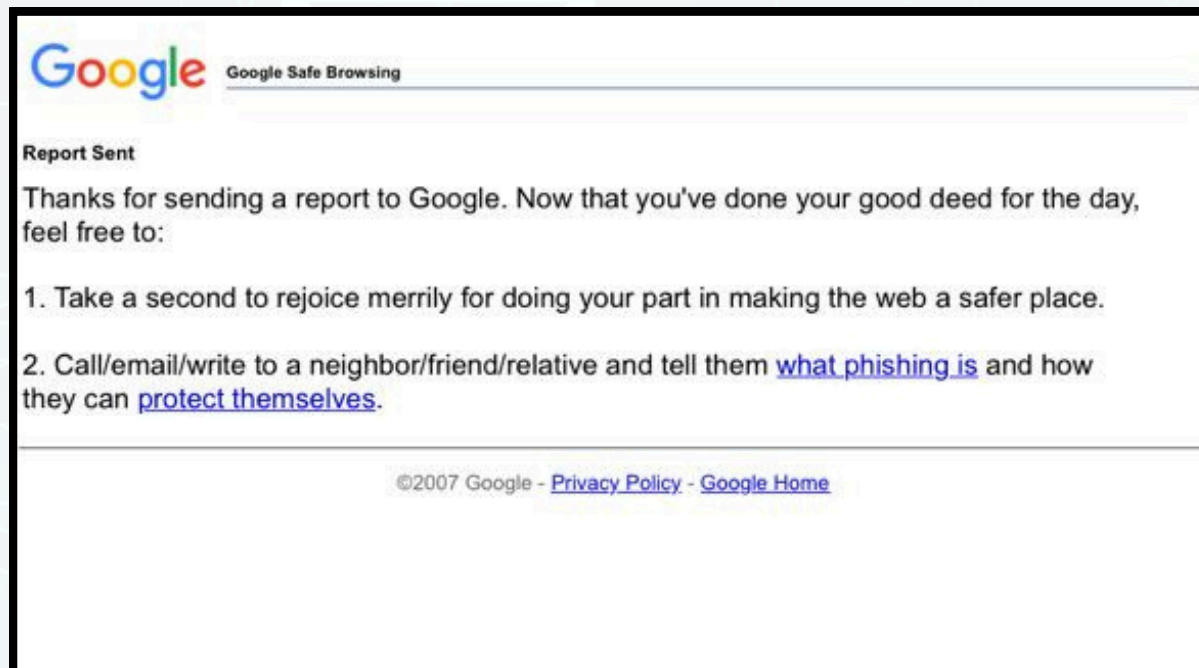
What time works for you tomorrow? I'll send you an invite for a zoom or google call.



Of course they weren't going to let me send them a meeting link, I wasn't going to send it anyway! This was the end!



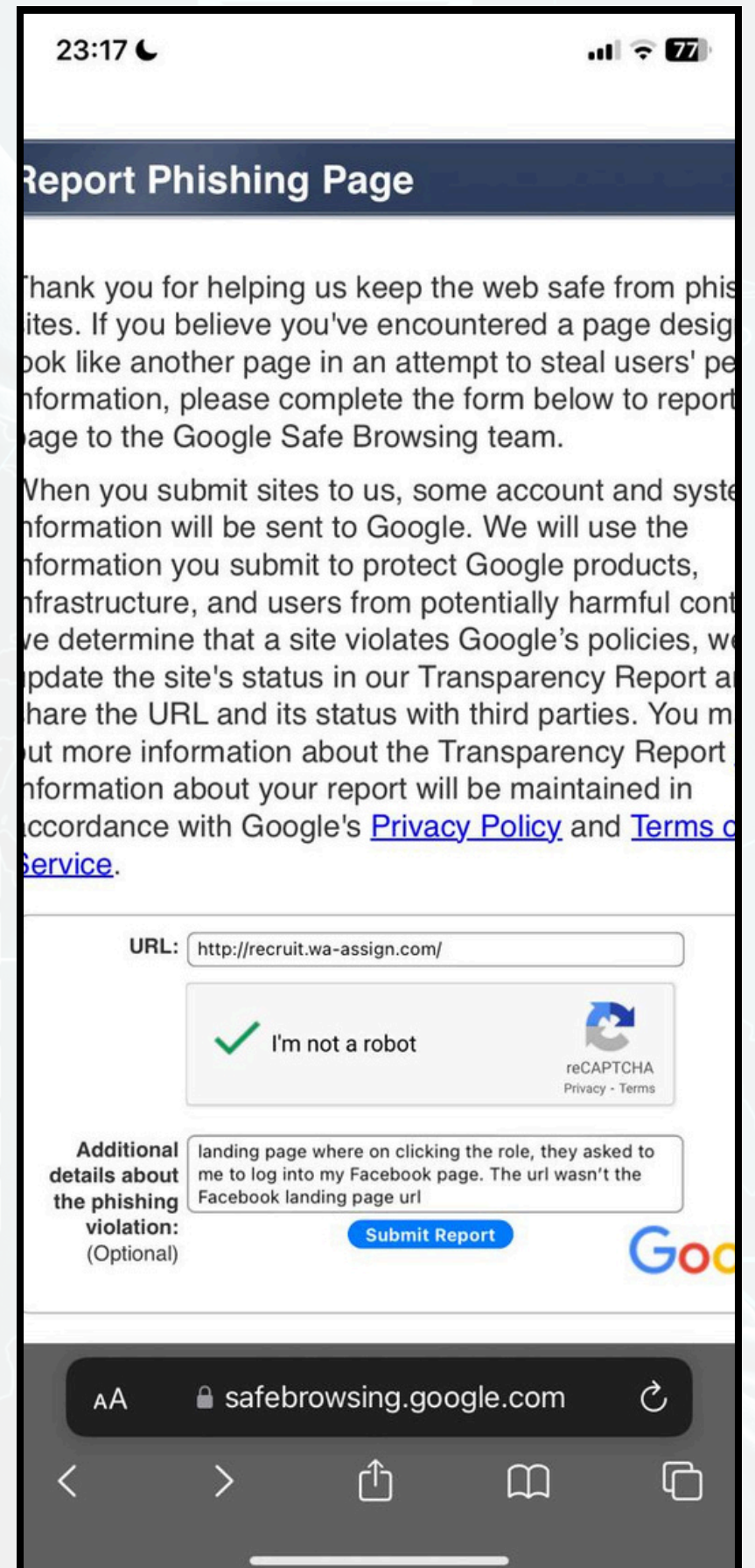
# What did I do following this?



I reported the link to Google, they have an anti-phishing page where you can do that.

Then I put these additional measures in place

1. Audited my account access, to see where I am logged in and which 3rd party apps have access
2. I double checked that I have 2FA activated everywhere
3. Deactivated the option where my LinkedIn connections could see my email address. I suspect this is where they got my email address from.





# It happens more often than you know!





# On 1st Feb 2025, hackers took over the Kenyan Government Owned TV station's account on 1st Feb 2025

## KBC Confirms X Account Hack, Name Changed to 'DeepSeek AI'



**UNDERRATED NINJA**   
[@iamjoseh\\_](#)

Follow

KBC Twitter handle has been hacked and handle changed to [@DeepseekOnSoI](#) 😂

21:57 · 31/01/2025 · **27K** Views


 37  170  341  21 

Most relevant replies ▾



**Mendy Fofana** [@mendy\\_fofana](#) · 10h  
Naona hadi wallet adress wameweka 😂😂😂


 1   9  2.4K 



**DeepSeek AI**  
[@DeepseekOnSoI](#)

Follow


Official DeepSeek Token [\\$DEEP](#) on Solana CA:  
6MGRnm24T71QKjinxoAc7hBBRzUNJp5ccF3iSjBApump

[deepseeksol.live](#)  Joined February 2011

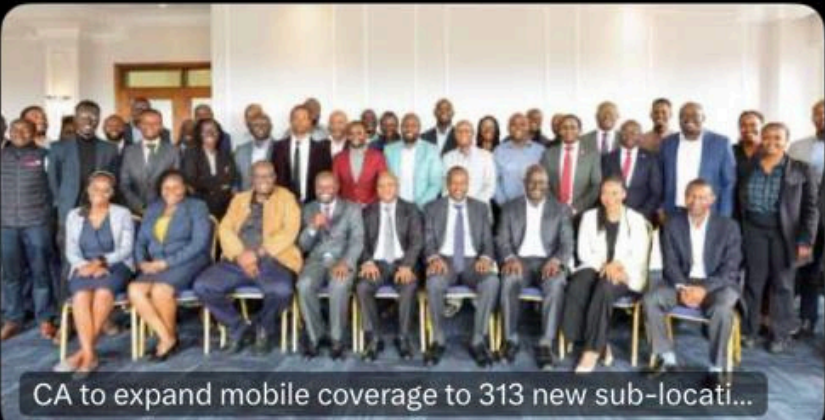
1.9K Following **897.2K** Followers

Followed by Maundu, Hon.Sumeya bishar, Bitdefender Kenya, and 160 others

**Posts** **Replies** **Highlights** **Media**



**DeepSeek AI** [@DeepseekOnSoI](#) · 25m  
CA to expand mobile coverage to 313 new sub-locations



CA to expand mobile coverage to 313 new sub-locati...

They even put a cryptocurrency wallet address in the accounts bio! Just incase KBC decides to pay the ransom to regain control of their account

# On 5th Feb 2025, hackers took over the X account of the MediaMax Owned TV station K24



K24 TV's X account (@K24Tv) was compromised, and we are working diligently to restore full access. We apologize for any inconvenience caused and urge caution when interacting with recent posts from the account.

In the meantime, please stay updated via our Facebook page: [www.facebook.com/K24Tv](http://www.facebook.com/K24Tv). You can also follow us on Instagram for the latest updates: @K24Tv

Thank you for your understanding and continued support.

5th February, 2025

k24.digital

X Accounts seem to be particularly vulnerable and media houses seem to be a HOT target! Hackers seem to be choosing globally trending names



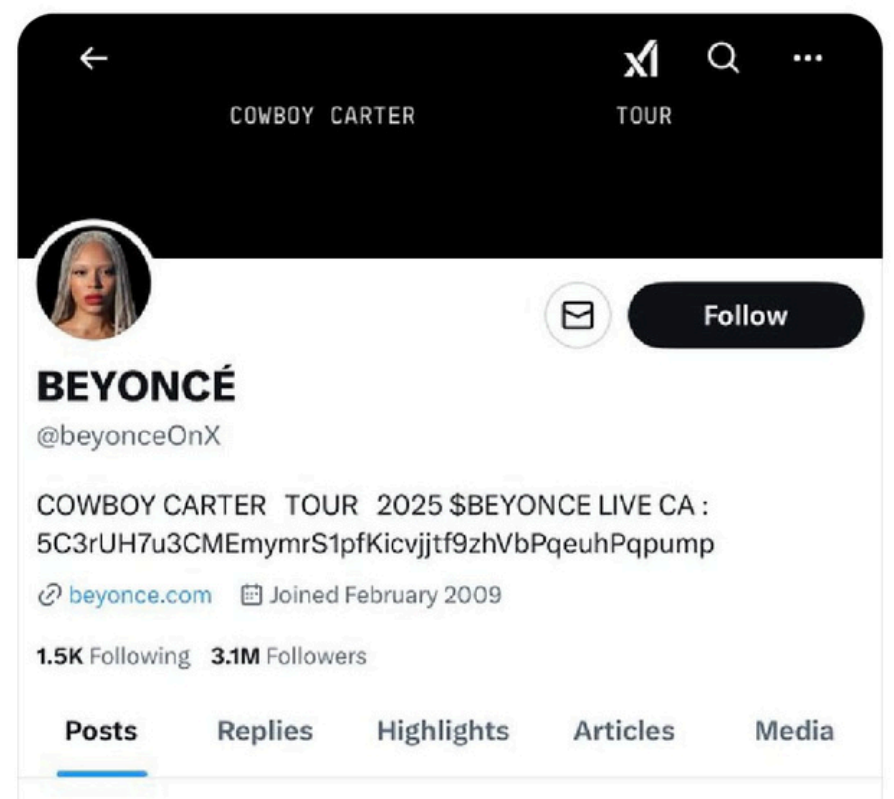
**Mastardcesh** @Mastardcesh · 51m

KBC account hacked last time and renamed Deep Seek

NOW

**K24** hacked and renamed Beyonce

Aura for Aura





# Prevention is better than cure

**Enable Two-Factor Authentication (2FA)** - Always use 2FA for Facebook and connected accounts. This adds an extra layer of security. The Google Authenticator app is another layer of security you can explore.

**Avoid Clicking on Suspicious Links** - Beware of emails or messages asking for login details, especially those claiming urgent account issues. Always verify URLs before clicking.

**Train your staff to identify phishing attempts** - 80% of organizations say that phishing awareness training helped them reduce the risk of their employees falling for phishing attacks

**Regularly Audit Account Access** - Periodically review who has access to your accounts and remove unused roles or third-party app permissions.

**Use Strong, Unique Passwords** - Create passwords that are hard to guess and never reuse them across accounts. Consider using a password manager for additional security.

**Stay Informed on Phishing Techniques** - Keep up with the latest phishing tactics. Platforms like Facebook often publish security updates to educate users about ongoing threats.

**Switch to managed Meta accounts** to reduce risks to your business account.

**Only load the funds you need on your media buying card** - This can be tedious and time consuming, but its the safe way to go about it.

# Other ways phishing attempts are happening now

## **Your Account Is Under Threat and will be shut down -**

These messages often come via Messenger. Facebook is quick to shut them down

**LinkedIn Messages** - These had started to pop up earlier in the year where new accounts would connect with you and send messages requesting for advertising services. Of course they would send links. LinkedIn seems to have shut them down. I haven't received any of late.

Text Message  
Mon, 27 May at 18:46

(Posta) Delivery is done 2/2 times,  
confirm your information or your  
item will be returned:  
<https://posta.com-co.top/ke>

Did you receive this  
message via text? Yeap,  
Phishing!





# STAY SAFE!



[www.torrasdigital.com](http://www.torrasdigital.com)

The strategy agency for digital led  
organisations



Digital Consultancy, training and talent recruitment