

# no go fall maga

THE HANDBOOK



CyberSafe Foundation



# no go fall maga

THE HANDBOOK



NFM  
NoGo  
FallBlago

No Go Fall Maga: The Handbook/CyberSafe Foundation  
Copyright © 2019 by CyberSafe Foundation

This publication is protected by International Copyright Law.

All rights reserved. The rights of the CyberSafe Foundation to be identified as the author of this work has been asserted in accordance with the copyright laws. No part of this publication may be reproduced, transmitted, or stored in a retrieval system, in any form or by any means, without permission in writing from the copyright holder.

**Bulk Order Information:**

Special discounts are available on quantity purchases by corporations, associations, and others. For details, please contact the publishers.

First Published, 2019

Designed and Published by:  
A'Lime Media Limited  
7, Anjorin Lane, Off Adegoke Street,  
Surulere, Lagos, Nigeria.

+234 901 000 0120  
[contact@alime.media](mailto:contact@alime.media)  
[www.alime.media](http://www.alime.media)

All images used aside illustrations in this book were downloaded from [www.google.com/images](http://www.google.com/images) and used under the Creative Commons License.

# no go fall maga

THE HANDBOOK





# Contents

Acknowledgments	ix
Foreword	xi
Introduction	xii
• The Outcome Was Not Income	16
• Everything Looked Right Until It Wasn't	20
• Literally Cashless	26
• Bundle of Loss	32
• Frank, The Scammed Guy	36
Activities	41 - 65
Activity 1: How To Enable Two-Step Verification On Whatsapp From An Android Device	44
Activity 2: How To Mitigate The Risk of Business Email Compromise Attacks	46
Activity 3: Phishing Test	48
Activity 4: Password Managers	50
Activity 5: Check If You Have An Account That Has Been Compromised In A Data Breach	52
#NoGoFallMaga	54



# Acknowledgments

**Book Cover Art:**

Toyin Paseda

**Contributors:**

Confidence Staveley, Simbiat Sadiq,  
Emmanuel Olaniyi, Ayodele Oluwatobi,  
Mubaraq Usman, Oluwatobi Towoju,  
Mohammed Okorejior, Ikechukwu Ani

**Stories:**

Olanrewaju Oladimeji  
for A'lime Media Limited

**Editorial Consultancy  
and Publishing:**

A'lime Media Limited

**Editor:**

Mirabelle Morah  
for BlankPaperz Media

**Illustrations:**

Ugo Jesse and Alvin Frezco

**Cover Art Direction:**

George Wonah

**Story Illustrations  
Direction:**

A'lime Media Limited

**Foreword:**

Remi Afon – President,  
Cyber Security Experts Association of Nigeria  
(CSEAN)



## Foreword

The search for an easy to understand cybersecurity awareness book has been on for a while, as readers find it difficult to understand what is required of them to stay safe online considering the ever-confusing advice from cybersecurity professionals and experts. "NoGoFallMaga," the author of this book has taken a different approach from the traditional prescriptive awareness campaign, to a more interesting and engaging style.

Smartphones, the internet, and social media have become a ubiquitous part of our lives today; these information technology tools and platforms offer numerous benefits and some downsides. The major downside is the exposure of end-users to a whole new range of cybersecurity threats and vulnerabilities. In most cases, we are not prepared or properly equipped to handle these threats, and some of us are not even aware that such threats exist. Cybercriminals are perfecting their methods daily, using the art of deception known as "Social Engineering" to exploit unsuspecting people on these platforms.

Cybersecurity awareness campaigns have been identified as one of the most effective methods to tackle cybersecurity related challenges. While the use of technology to curtail cybersecurity threats are being adopted by a lot of organisations, unfortunately, it is inadequate without user awareness campaigns. Research shows that the most effective form of attack on the security infrastructure of any organisation, is through the exploitation of individuals; which is why experts say cybersecurity is not just an IT issue. The

technologies deployed are only as good as the users.

This book is designed to provide the necessary insight to help individuals and organisations alike, to understand the techniques that cybercriminals can adopt in exploiting unsuspecting victims. The book provides a series of storylines that take the reader through the journey of how easily one can fall prey to cybercriminals, thereby changing the mindset of readers to a more security conscious one in a subtle way.

Eleanor Roosevelt, the wife of former American President, Franklin D. Roosevelt, once said: "Learn from the mistakes of others. You can't live long enough to make them all yourself." Thus, being a victim of cybercrime is not palatable, and it is not something you may want to experience.

In my several years as a cybersecurity consultant, I have read a lot of cybersecurity awareness books of which most are very confusing to say the least, due to too much technical information. However, this book relates directly to everyone irrespective of technical background. It is fun to read. The combination of games, infographics, and calls-to-action make learning easy and comprehensible. "NoGoFallMaga" is one of the leading cybersecurity awareness campaign groups in Nigeria and has painstakingly taken cybersecurity awareness to another level with this book. This is a must-read for everyone who wants to stay safe and secure online.

Remi Afon  
President  
CSEAN

## Introduction

The 2018 Nigeria Cybersecurity Outlook report, published by Deloitte, revealed that social engineering attacks (the art of convincing people to reveal confidential information) which are conducted via emails, SMS and telephone calls, were the number one cyber threat in Nigeria. Interestingly, the 2019 version of the same report predicted that the year 2019 would witness sophisticated phishing attacks with social engineering-themed messages targeting all sectors. In fact, Bulent Teksoz of Symantec Middle East noted that, "Cybercrime is shifting towards the emerging economies. This is where the cyber criminals believe the low hanging fruit is." So far, these predictions have been apt. In 2017, Nigeria's estimated losses to cybercrime was a staggering \$649 Million. Today, the cyber-victimization rate in Nigeria continues to increase as home-grown cybercriminals, ever more than before, are looking inwards for targets.

Also, in today's cyber threat landscape, every organization, regardless of size is at risk of an attack. Although small and medium businesses are the focus of attacks, they also often serve as launch pads or conduits for bigger attacks targeting larger enterprises.

Interestingly, most SMEs in Nigeria lack the following: a functional IT Department with in-house cybersecurity expertise, a budget for cybersecurity solutions or both.

While social engineering has been in existence for a long time, the pervasive, ubiquitous and innovative use of technology by businesses as well as perpetrators, has amplified the effectiveness of this dangerous strategy. The intriguing concept about social engineering is that there is no single technology solution that can guarantee 100% protection of employees from these types of attack. The most effective preventive solution remains the education of employees, thus, enabling them to recognize and respond appropriately to social engineering attacks.

Taking a storytelling approach, we aim to bridge cost barriers of access to cybersecurity awareness training for SMEs and enhance the employee learning experience. Consequently, we have delivered a fun, engaging and highly educative handbook about the evolving social engineering tactics deployed by fraudsters and hackers in Nigeria.

We do not attempt to address all cyber threats that businesses may face; we have narrowed our focus to cyber threats that originate from successful social engineering attacks. With each story, we empower and raise awareness on every tech-user's role in ensuring that a good cybersecurity posture is maintained in any organization. We emphasize that cybersecurity is not the responsibility of an IT department only because personal cyber safety and that of every organization, hinges on the decisions made every day, as humans interact with technology.

We are therefore pleased to present Africa's first storified Cybersecurity Awareness Training Handbook designed for SME entrepreneurs and employees, by #NoGoFallMaga.

Confidence Staveley  
Founder  
#NoGoFallMaga

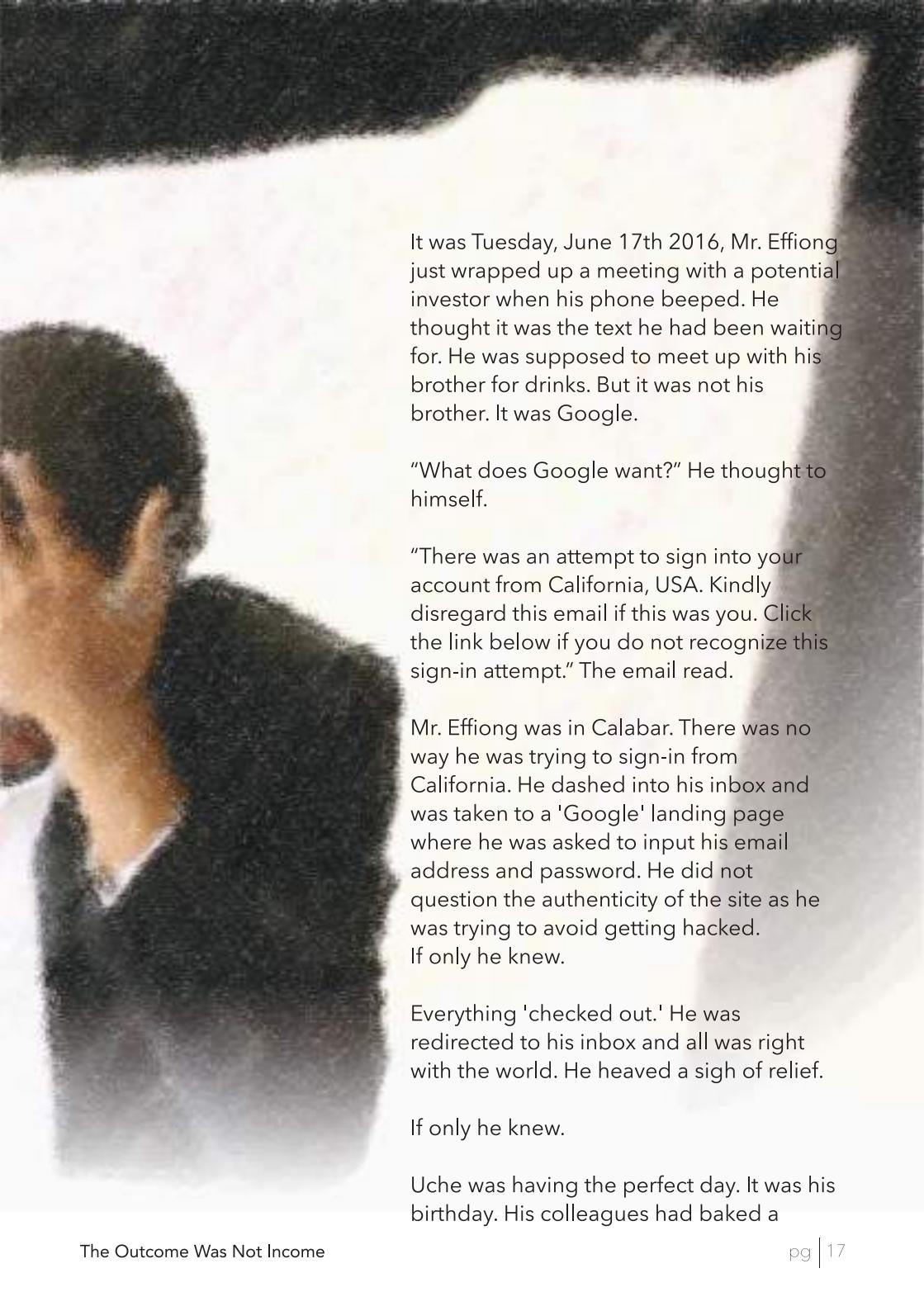


# the outcome was not income

He got fired over something he could have avoided.

Uche worked for a Microfinance bank in Ikot Ishie, Calabar. A city known for its rich culture, tourism and people. Uche was extremely diligent in his work. He came in as an intern but quickly rose to become one of the most important members of the finance team.

KT Microfinance Bank started in 2013 and had quickly grown to become one of the biggest micro-finance banks in Calabar. Their customer service was second to none. All thanks to the introduction of the new General Manager, Mr. Okorn Effiong. Mr. Effiong was stern. He believed the customer, the heart of a business, is king and would do anything to please even the 'littlest' customer. He instilled this attitude in the hearts of all staff, and this made IKT Microfinance Bank outshine its peers.



It was Tuesday, June 17th 2016, Mr. Effiong just wrapped up a meeting with a potential investor when his phone beeped. He thought it was the text he had been waiting for. He was supposed to meet up with his brother for drinks. But it was not his brother. It was Google.

"What does Google want?" He thought to himself.

"There was an attempt to sign into your account from California, USA. Kindly disregard this email if this was you. Click the link below if you do not recognize this sign-in attempt." The email read.

Mr. Effiong was in Calabar. There was no way he was trying to sign-in from California. He dashed into his inbox and was taken to a 'Google' landing page where he was asked to input his email address and password. He did not question the authenticity of the site as he was trying to avoid getting hacked. If only he knew.

Everything 'checked out.' He was redirected to his inbox and all was right with the world. He heaved a sigh of relief.

If only he knew.

Uche was having the perfect day. It was his birthday. His colleagues had baked a

beautiful cake for him and nothing could go wrong. Well, so he thought.

He sat at his desk chewing his cake mildly while going over his emails to see if he had any unread messages before shutting down for the day. But then he received a notification. It was the general manager, Mr. Effiong. And it was an emergency. Mr. Effiong was leaving the country and needed funds to book his ticket and also make immediate purchases. It did not sound like Mr. Effiong. The urgency was suspicious and the account details he was to transfer funds into did not have Mr. Effiong's name. But then, Mr. Effiong was a stern man who didn't like being queried, or so Uche thought. Also, it was extremely time-bound and so, there was no time for 'due-process.'

Uche immediately authorized the transfer of money to the account that was sent to him and went home. He had the perfect day.

If only he knew.

Uche showed up to work the next day and was thrown aback when he saw Mr. Effiong.

"He's supposed to be out of the country!" He mumbled to his colleague.

"He wants to see you in his office." His colleague replied.

Uche could sense what it was about.

"Who authorized this transaction!!" Mr. Effiong screamed.

Uche tried to explain himself. He had sent the money so he, Mr. Effiong, could buy his ticket and the other things he mentioned.

"My goodness! You authorized the transfer of 1 Million Naira to an account that did not have my name on it without checking with me first?" Asked Mr. Effiong, furious.

Mr. Effiong spent minutes schooling him on the million ways it could have been avoided.



“You should have called me to confirm the account details when you noticed the urgency in my tone and the mismatching account details. That should have been a red flag for you. Speaking of which, don't we have measures and policies regarding transfers above a certain amount? You should have observed due-process but instead, you decided to be judge and jury. Now this company just lost 1 Million Naira due to your negligence!

“You should have called me to confirm the account details when you noticed the urgency in my tone and the mismatching account details. That should have been a red flag for you. Speaking of which, don't we have measures and policies regarding transfers above a certain amount? You should have observed due-process but instead, you decided to be judge and jury. Now this company just lost 1 Million Naira due to your negligence!

“You're fired! Leave your things on your desk. The security men will escort you out and you'll be hearing from our lawyers.”

Uche was speechless.

“T-t-they sent the email using your gmail account, sir. I thought it came from you...” Uche tried to get the words out while weeping profusely.

Mr. Effiong was guilty of one thing, not vetting the link he clicked on and also giving out his credentials without proper due diligence.

Everything they thought was right, was wrong.

If only they knew.

# everything looked right until it wasn't.

**B**usiness has been extremely slow for a lot of small scale entrepreneurs in this country. The cost of entry is burdening. Sustaining it is another headache. You have to worry about lots of overhead costs especially with the epileptic power supply in the country. Fuel costs keep spiking, materials for businesses are getting scarcer and scarcer, and when they eventually become available, the prices are overwhelming!

Tayo, one of the many entrepreneurs in the makeup industry, was lamenting to a friend who came to her shop. The makeup industry had become overly saturated. Everyone with a foundation and concealer seemed to change their Instagram bios to "Your favourite MUA."



"Who are they fooling?! My dear, these quacks are ruining the market for we wey sabi!" Tayo lamented. Everyone wants to get a full makeover at almost no cost and it's because certain 'quacks' have crashed their prices.

"The real ones that know our worth are still calling us o jare." Tayo bragged as she let out a sheepish grin.

They went on about work, nagging customers, the men in their lives and parties they had to attend. Lots to talk about. Her friend left and Tayo was back to her shop, dealing with more bookings. The business was booming and she couldn't be happier.

Everything was going right.

It had been an extremely busy week for her as she had a lot of calls and emails coming in. It was the festive season. Lots of parties. That only meant one thing – lots of makeovers to be done. She couldn't be mad at that.

Her phone rang. "Another real one," she assumed wrongly. It was her bank and she could tell from the caller ID. She had called them a thousand and one times so she already knew the number by heart. They would put her on hold for minutes so she would put the phone on speaker and randomly call the numbers out. That was how she passed time. She was surprised they were calling her because unlike before, she didn't have any new complaints to make to them. That rarely happened as she had contemplated closing her account with them countless times due to the herculean task of having to go to the bank every time she had a complaint. She could not fathom how in this digital age, she could not sort things out over the phone or via email.

Tayo might have been busy, but a call from her bank was something she wouldn't miss. She immediately answered the call. The customer care representative from her bank introduced herself as Lydia and got right to the point.

"Madam, is your name Tayo Ogunnaike with account number 0975672231?"  
"Yes, that's me, is there a problem?" Tayo responded.

"Madam, we noticed a discrepancy on your account. Your internet banking details look compromised. We sent an email to you but we have not gotten feedback from you. Kindly check your email and follow the link we sent to you to create a new password as soon as possible. It's very important."





Tayo was in the middle of work and hearing she had a potential account compromise on her hands was enough to send her into a frenzy.

"Okay... Okay... I'll check and revert... Thank you!" She said as she hung up.

She ran to her laptop and fired up her gmail and there it was, an email from her bank. Again, the email address checked out. She had received several emails from that account. She was certain it was her bank. She clicked the provided link and was redirected to a landing page to fill in her user ID and create a new password.

Everything looked right.

She was too busy to ask questions. She just wanted to get it over with and get back to work. She filled in her details, created a new password and hit the submit button.

All was right with the world again. So she went back to work. Then barely an hour after, the first debit alert came in – 35,000 Naira! Then the next and the next one after that.

Tayo couldn't understand what was going on and so, she called her bank

**Tayo couldn't understand what was going on and so, she called her bank immediately. She tried explaining to the customer care representative what had happened; how she had been contacted by a lady from their office earlier on, and how she had changed her password.**

immediately. She tried explaining to the customer care representative what had happened; how she had been contacted by a lady from their office earlier on, and how she had changed her password.

"Madam, we would never ask you to give us your private information. I am looking at our records right now and no outgoing calls to you have been made. Kindly confirm the call came from us," he responded.

It was then it dawned on her. She had been scammed.

Everything checked out. It was the same number she was used to. The website she was redirected to was a mirror image of what she knew. How could this be?

Then she remembered: there was an urgency in that call. The lady she spoke to kept emphasizing she needed to respond immediately. That should have been a red flag. But then, personal data? Why was her bank asking for her personal data? She should have known.

She reminded the customer care representative that the number checked out. It was then he gave her the lecture about call spoofing.

"Madam, the number appeared as though it came from us but it in fact, was not. There are apps and websites these hackers use to mirror phone numbers so that unsuspecting recipients of these calls fall victim because the number checks out. Most of these calls are made over the internet so it's usually difficult to trace. Please, note that we would never request for your personal details. This should be a red fl..."

Tayo hung up the phone without letting him finish as she screamed her own "I'm finished!"

# literally cashless

Technology is amazing!

It has changed so much for a lot of people. A whole lot of people!

Some people would argue it has made everyone lazy. Here's why. We are in the cashless era. No one carries money around anymore. Card payments are the way to go! The joy when you can just swipe to pay is immeasurable. You mean people don't need to carry wads of cash around anymore? We don't have to worry about getting robbed? Our pockets can be lighter when we move around?

If that isn't bliss, nothing else is!

If you think that is as far as bliss goes, then you obviously have not gotten on the eCommerce wave. eCommerce has changed everything. So, people can avoid all that market stress and sit behind their phones or computers and shop? My goodness!

eCommerce has had a tremendous impact on the business landscape in Nigeria. Still not convinced, out of over 180 million people in the country, 62% are youths. Nigeria also ranks 7th place on the list of countries with the

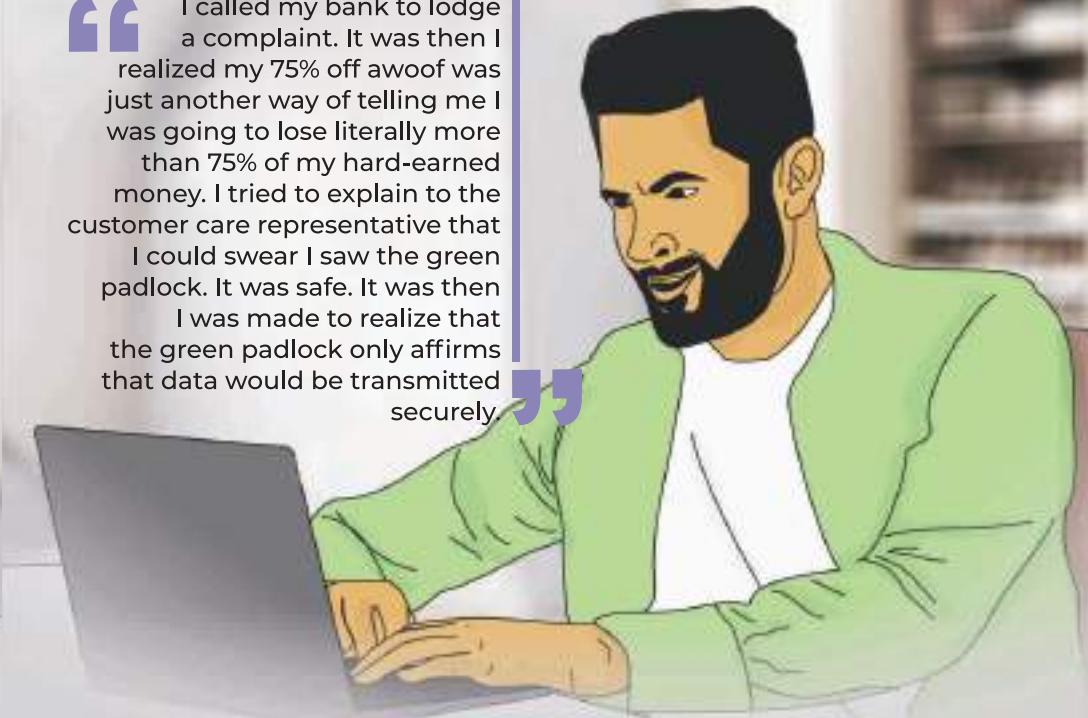


most internet users. Considering the number of youths and individuals that have access to the internet, this presents a gold mine for businesses. The internet is the place to be. eCommerce is the way to go!

I am one of those youths who actively champions the cashless and eCommerce story. I can't remember the last time I was in a physical store. If it's available in a physical store, there is an online marketplace and that's where I will rather be. Miss me with that physical store stress. I can't be letting indisciplined men pull me from all sides trying to get me to buy from them. Traffic in Lagos is another discouraging thing. What I do is go online and get my items. Works all the time!

I've always been a sucker for deals. Black Friday deals, discount sales, buy one get one free offers and all. I was always on the lookout for cheap products or incentives. I always wanted more, as the typical Oliver Twist that I was. But I learnt my lesson the hard way.

“ I called my bank to lodge a complaint. It was then I realized my 75% off awoof was just another way of telling me I was going to lose literally more than 75% of my hard-earned money. I tried to explain to the customer care representative that I could swear I saw the green padlock. It was safe. It was then I was made to realize that the green padlock only affirms that data would be transmitted securely ”



Let me let you in on something, you know that line, “not all that glitters is gold.” That's my new mantra. It's the gospel.

I was in one of my shopping spree modes. Adding any and everything that looked good to my cart. Grinning at pretty items and mentally simulating how I looked in the dresses I was selecting. Of course, I was not going to buy those things immediately. Not until it was Black Friday again. I just added them to my cart so I would initiate checkout once it was time; Black Friday time!

My awoof self was running wild. I spent more time searching for cheap products or websites that offered discounted products. It was taking forever to get and I was starting to give up when I saw the link – 75% off all purchases between now and midnight.

“Haq Haq Haq!”

75%. I calculated all the things I could buy with that. I couldn't count. Perfect!

I clicked on the link and was introduced to an aesthetically appealing landing page with well-segmented products. I was too carried away with how eloquently furnished the site was. Products sat pretty in their slots with goods originally costing 40,000 Naira slashed to 10,000 Naira.

It was too good to be true but there it was, staring at me. I looked at the address bar and saw the green padlock. I reassured myself it was real.

I filled my cart with all the things I had always wanted to get and proceeded to checkout. I kept glancing at the address and every time I saw the green padlock, I told myself all was well. I inputted all my details, including my card details made payment and hoped I got my products on time. They were true to their words. It took seven days as promised but it came. I was excited. We would definitely be doing more business together. I wasn't done with them.

Well, they weren't done with me either.

The debits kept rolling in. I had no idea what was going on. I was losing money fast. The debit alert was telling me I was making purchases on foreign online stores. I loved to shop but that wasn't me.

I called my bank to lodge a complaint. It was then I realized my 75% off awoof was just another way of telling me I was going to lose literally more than 75% of my hard-earned money. I tried to explain to the customer care representative that I could swear I saw the green padlock. It was safe. It was then I was made to realize that the green padlock only affirms that data would be transmitted securely. It is not a guarantee that the vendor is genuine. He explained that the 75% off purchases made, was an offer that was too good to be true and it was a technique used by online scammers to lure overly enthusiastic shoppers to give up their card details which would eventually be used to make purchases on their behalf or be sold off on the dark web. The shoppers would get their orders but would lose much more. I had gained a few products but lost all my money.

Awoof really dey run belle.

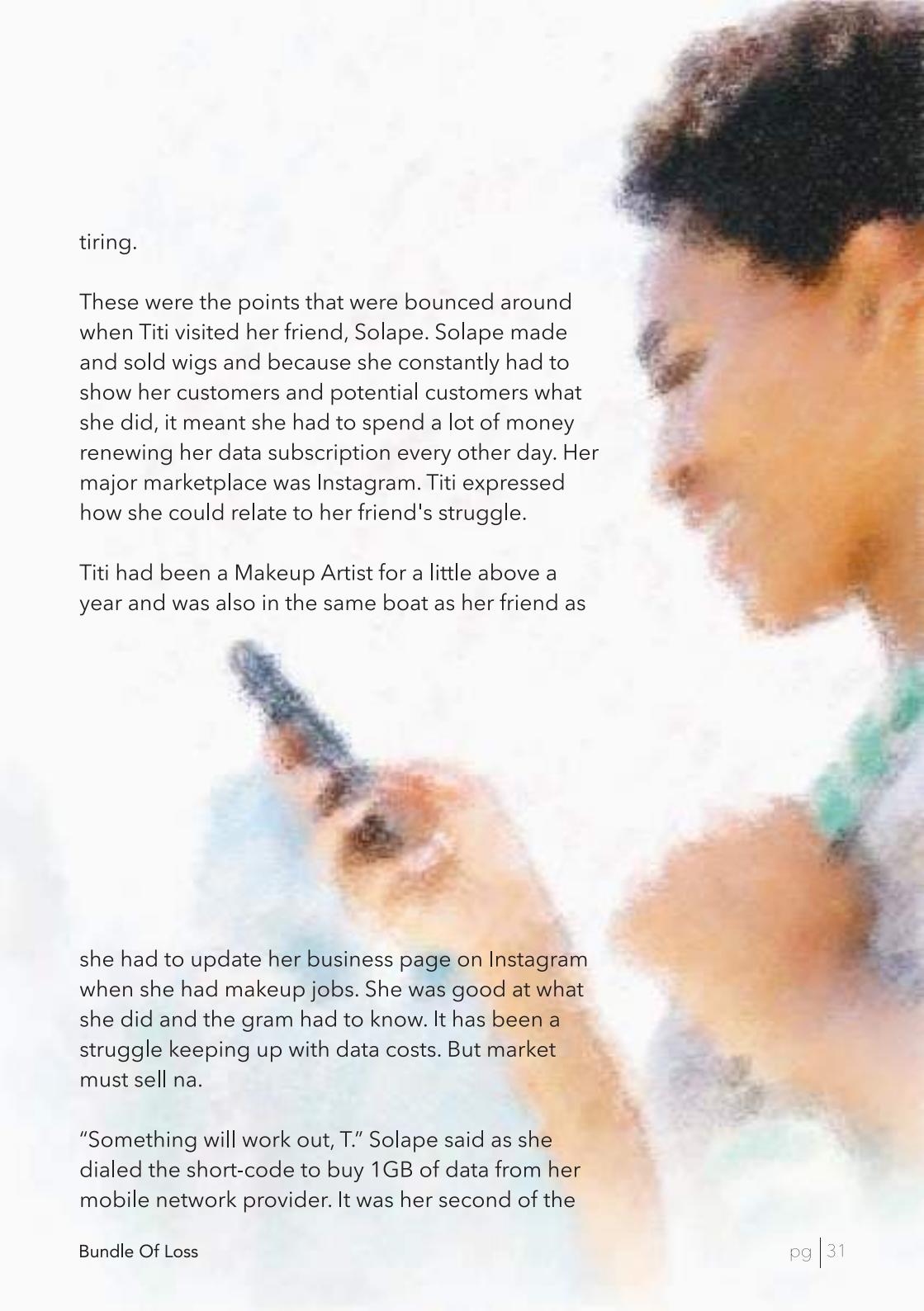
# bundle of loss

Data is life! It is literally what gets most of us through the day. Data controls what we see, read or watch on the internet every day.

How accessible that data is, is another question on its own. Even more pertinent is the cost of what's accessible. Data costs are extremely high and this poses a serious threat to individuals looking to stay updated on happenings on the internet. Businesses are not left out as they are majorly the ones with much to lose, especially businesses heavily dependent on the internet to function.

**B**ig businesses can foot the bills effortlessly, perhaps. Small businesses on the other hand are left to count their losses most times due to huge overhead costs in running their businesses. Costs ranging from salaries, fuel to data.

The complaints usually range from the high data cost to the rate of exhaustion. 1GB is the new 1MB. It's insane. The WiFi providers weren't helping matters also. They were highly overpriced. They also promised unlimited data which in actual sense was not unlimited but had a cap. It was



tiring.

These were the points that were bounced around when Titi visited her friend, Solape. Solape made and sold wigs and because she constantly had to show her customers and potential customers what she did, it meant she had to spend a lot of money renewing her data subscription every other day. Her major marketplace was Instagram. Titi expressed how she could relate to her friend's struggle.

Titi had been a Makeup Artist for a little above a year and was also in the same boat as her friend as

she had to update her business page on Instagram when she had makeup jobs. She was good at what she did and the gram had to know. It has been a struggle keeping up with data costs. But market must sell na.

"Something will work out, T." Solape said as she dialed the short-code to buy 1GB of data from her mobile network provider. It was her second of the

day. 1GB cost her 1,200 Naira.

Solape and Titi both belonged to a WhatsApp group, Lagos Businesswomen, where small businesses like theirs came together to share ideas, opportunities and network with each other. They would exchange banter once in a while and anyone who had a customer asking for something they could not provide, they would refer to someone else on the group that could. It was a family.

Once Solape's internet connection was restored, the messages kept rolling in. Her Instagram DM was buzzing with "how much is this?" questions. Her WhatsApp wasn't left out. It felt like she had been away forever. The notifications wouldn't stop. Half of those WhatsApp messages came from one place, Lagos Businesswomen.

"What are these ones always saying gan."

You could sense the frustration in her tone. She opened the group page and scrolled through the



Once Solape's internet connection was restored, the messages kept rolling in. Her Instagram DM was buzzing with "how much is this?" questions. Her WhatsApp wasn't left out. It felt like she had been away forever. The notifications wouldn't stop. Half of those WhatsApp messages came from one place, Lagos Businesswomen.

messages. She was right. It was all banter until she hit a screenshot with a caption "come and see o!"

She clicked the image and let out a grin.

"Titi come and see what Chichi posted!"

The text on the image read:

"Exclusive Data from a reliable seller. We work 24/7 and give the best rates.  
Call 08101220912 See our prices below..."

#### MTN DATA BUNDLE

3GB = #1000

4.5GB = #1500

10GB = #4000

....."

That was all she needed to see. The solution to all her troubles.

Before Titi could get words out, Solape was already dialing her new plug's number. At the end of the phone was a stern male voice reassuring Solape that he was legit. He told her the validity period was 90 days and tried to convince her that compared to other vendors, this one would last very long. It was cheap and it would last.

Those were the words she wanted to hear. Anything to smoothen her business operations.

She asked how it worked and that's where things started getting tricky.

He told her she would soon receive a verification code and she



“ He told her she would soon receive a verification code and she was required to forward that code to him so he could register her sim card on a platform that would enable her to have access to the cheap data plans, and also prevent her subscription from expiring prematurely.

was required to forward that code to him so he could register her sim card on a platform that would enable her to have access to the cheap data plans, and also prevent her subscription from expiring prematurely.

“Okay, I just received the verification code. So, I should send it to you abi?” Solapo asked.

“What code?! Don't send any code to anybody o!” Titi screamed from where she sat.

Before Solape could respond, she heard her caller let out a long hiss before he hung up the phone.

"Solape, don't you know that's how these nonsense scammers behave? Which yeye platform is he registering you on that he is asking you to send a verification code? Don't you know he was trying to gain access to your account? That code he was asking for is the one WhatsApp sends to verify your number na." Titi explained.

"Ah, I didn't know o!" Solape was embarrassed. How could she have been so gullible?

Titi went on.

"To make matters worse, they would then implement two-factor authentication so you can't gain access to your account anymore. Once they gain full control of your account, isallover! They pose as you and defraud people on your contact list. See, don't share any verification code with any one. No matter what and implement two-factor authentication on your WhatsApp. In fact, bring your phone. Let's do it now! Mumu."





# frank, the scammed guy

Frank went back to search for more. He was not satisfied. He wanted more and he would not stop until he had applied for everything possible.

\*\*

Frank was an industrious man. He worked as a business analyst for a multinational. He was highly passionate about business processes and business reengineering. He read lots of business-related books and could not stop attending conferences. Those were some of the ways he networked and met new people. He was a sucker for building relationships and he did a good job at doing that.

He was active on social media as well. He belonged to suit and tie Twitter. You know those guys who only share business opportunities, vacancies and make threads about enhancing your curriculum vitae or how to grow your business? Those guys. He tweeted a lot, but never about the things that didn't matter to him. Frank was the guy to tag when you needed business-related information.

It was not long before Frank found a new passion – online scholarships. Frank studied Mass Communication at the University of Abuja and since then, he had amassed lots of online certifications. It was time to take it a notch higher. He needed a Master's Degree from a foreign university.

He started to research online scholarship programs. From Mandela Washington Fellowship to the British Chevening Scholarship. He applied to everything within his purview. He was passionate about the growth of businesses and he pursued that vigorously.

None was forthcoming at the time but he wasn't one to give up. He kept pushing.

Frank constantly updated his online followers about his successes and failures at pursuing an online scholarship program. His aim was to motivate his followers and it was working. He got a lot of "I'm inspired by your hustle" related tweets and feedbacks. He wanted to do more and he did much more.

Frank was at home carrying out his usual scholarship research when he received an email.

What caught his eye was the subject of the email: "International Business Developers Conference 2019."

"That's interesting." He thought to himself as he opened to read the body of the email.

"Dear Sir/Madam,

On behalf of the Business Analyst and Developers Association (BADA), we are pleased to invite you to attend the international business developers conference which will be taking place from November 25th to 30th 2017, at Golden William Hotel situated in Dallas, Texas USA.

The theme of the conference is "Risk Assessment and its Impact on Startup Growth." The sponsors of this event shall cover your round-trip flight tickets from your country to the USA and back to your country, and we shall also provide visa assistance with the U.S Embassy in your country of residence.



“ Frank constantly updated his online followers about his successes and failures at pursuing an online scholarship program. His aim was to motivate his followers and it was working. He got a lot of “I'm inspired by your hustle” related tweets and feedbacks. He wanted to do more and he did much more. ”

The hotel accommodation booking cost will be your responsibility. Please contact the conference secretariat for more information and registration for participation: [bada.officeinfo@aol.com].

We look forward to your confirmed presence at the conference.

Respectfully Yours,

Jake Wright

Programs Assistant."

Frank could not believe his eyes. Did he just get an invite to the United States? His dreams were becoming a reality and he didn't know how to hide his excitement. He had always wanted to attend the International Business Developers Conference.

He responded to the email immediately stating his interest to attend and inquiring about next steps.

He got a response reassuring him of his slot, but warning him to book his hotel reservation on time as limited slots were available and people were making payments quickly. His passport number and other personal data were requested. The urgency spurred Frank to make immediate payment. The urge to be a part of the conference prevented him from thinking straight. He supplied all the information asked of him without question.

The thread went cold.

Days passed. Frank sent countless emails. He got no response.

Then he did something. Something he should have done from the beginning. He recalled an article he read on [www.opportunitydesk.org](http://www.opportunitydesk.org) about how hackers prey on unsuspecting victims by posing as conference organizers.

"Could it be..." He held onto that thought and ran a background check. Frank searched the name of the program assistant that emailed him and cross-referenced it with the actual name of the program assistant for the Business Analysts and Developers Association. It didn't check out.

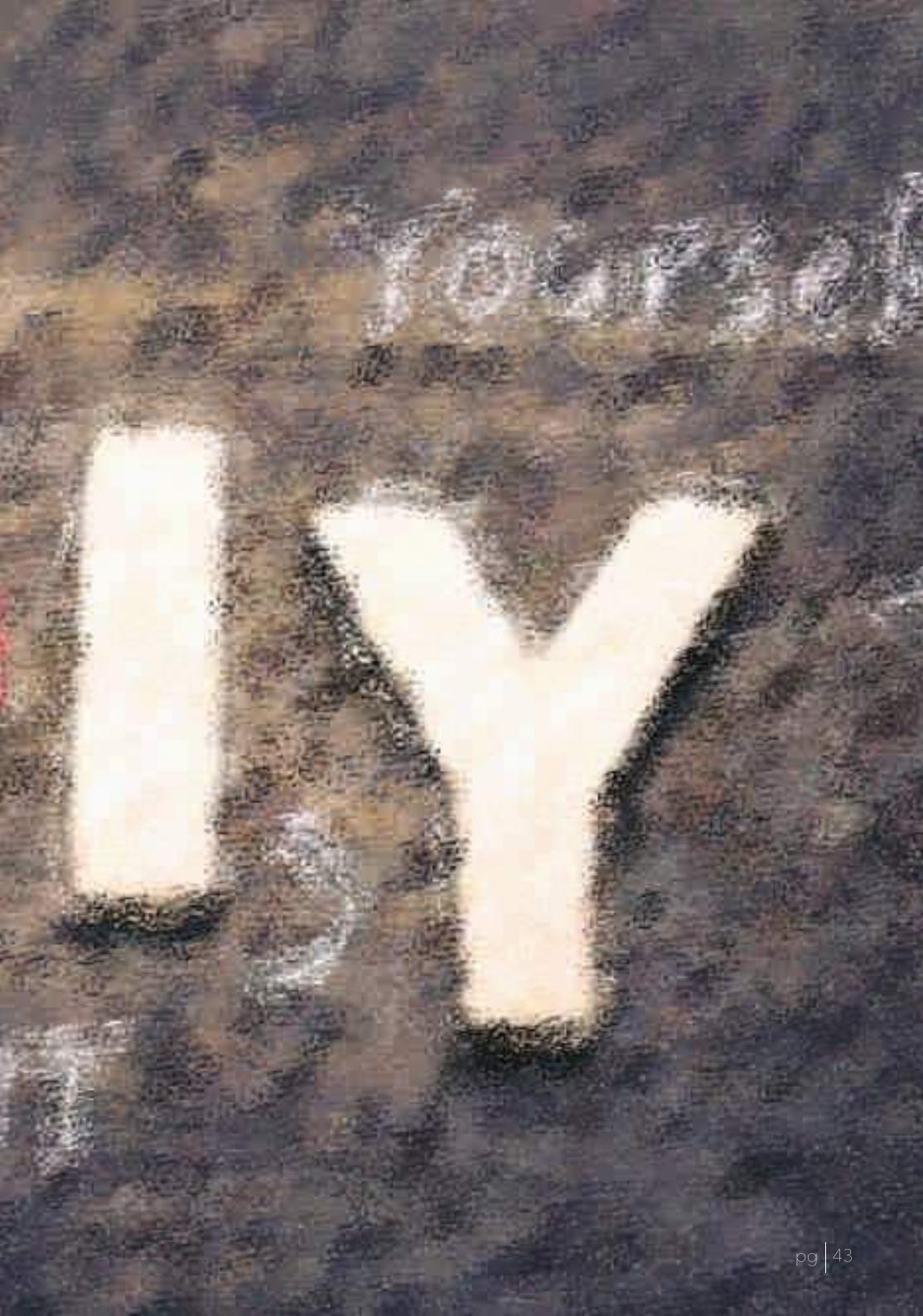
The conference he was supposed to be attending was not scheduled to hold in Dallas. It was scheduled to hold in Washington D.C.

Frank could not believe his eyes. He had lost \$600 to scammers! His excitement got the best of him and he failed to do a background check. He also failed to realise it was odd for a conference of that magnitude to request for payment via emails.

Frankly, Frank could have been wiser.

Frank could not believe his eyes. He had lost \$600 to scammers! His excitement got the best of him and he failed to do a background check. He also failed to realise it was odd for a conference of that magnitude to request for payment via emails.





## ACTIVITY 1:

# how to enable two-step verification on whatsapp

from an  
android  
device



## Activities



### for more information

on how to setup 2-FA for WhatsApp, Instagram, Facebook and Twitter, please visit [www.nogofallmaga.org](http://www.nogofallmaga.org).

## ACTIVITY 2:

# how to mitigate the risk of business email compromise

**Be Aware of Common Scenarios:**

Cyber criminals often rely on certain tactics to perpetrate business email compromise. To stay protected, concern yourself with how these attacks happen.

**Train Employees to Recognize BEC Attacks:**

Provide employees with adequate cybersecurity training and foster a sense of responsibility throughout the organization. Conduct user training on BEC threats, especially on how to identify spear phishing emails.





#### Create a Culture of Compliance:

Training and compliance need to go hand-in-hand to thwart BEC attacks. An effective compliance culture supports employees with the protocol they need to follow.

#### Implement Multi-layered Technological Defence:



Leverage technology to enforce controls, filters, preventive and detective mechanisms for BEC attacks. Consider adding an email banner stating when an email comes from outside your organization so they are easily noticed.



#### Enforce Multi-channel Conversation Authentication for all Payments and Financial Records Change Request:

Contact requestors by phone before complying with e-mail requests for payment or personnel records changes. Ensure company policies provide for verification of any changes to existing invoices, bank deposit information and contact information.

#### Optimize Accounting Systems and Process Controls:



Create payment approval processes and controls that create checks and balances, removing veto power.



#### Frequently Test Your Procedures and Processes for Exploitable Loopholes:

Consider setting aside a budget to hire penetration testers. These professionals will perform social engineering tests on your organization to highlight system loopholes and provide possible fixes.

## ACTIVITY 3:

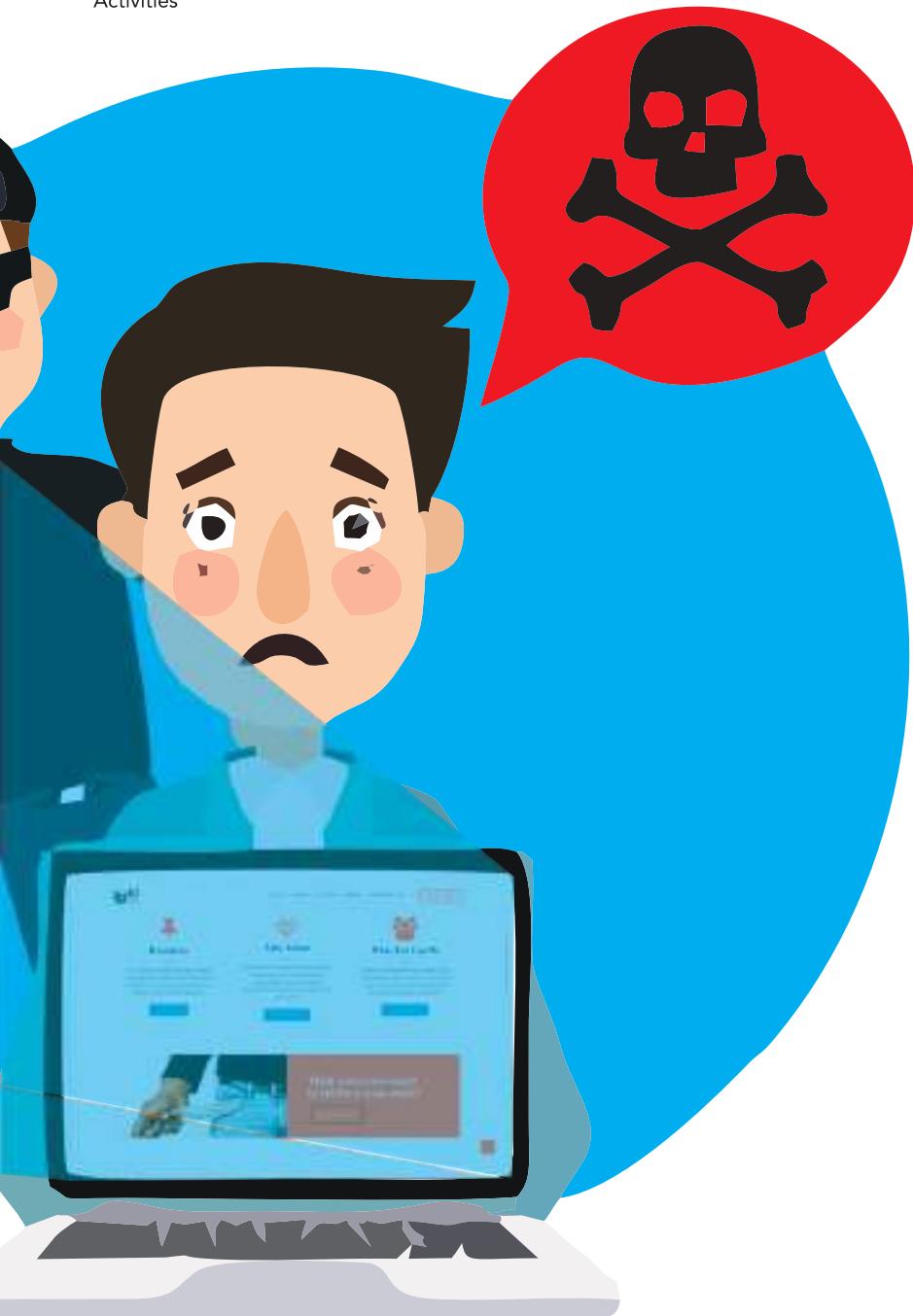
# phishing test

The screenshot shows a website layout with a navigation bar at the top featuring links for NEWS, STAFF, ACTIVISMS, MEDIA, and CONTACT US, along with social media icons. Below the navigation, there are three main sections: Resources, Take Action, and What You Can Do. Each section has an icon (red pin, red hands, red person), a title, and a brief description. At the bottom of the page, there is a large image of a person's hand reaching into their pocket, with a red overlay containing the text "Think you're too smart to fall for a scam email?" and a "TAKE THE TEST" button.

**Think you're  
too smart to be  
scammed?**

Visit [www.nogofallmaga.org](http://www.nogofallmaga.org)  
to take a phishing email test.

## Activities



## ACTIVITY 4:

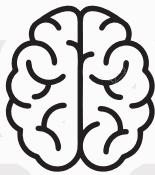
# password managers



- LastPass
- Dashlane
- 1Password
- ZohoVault
- KeepPass

A password manager is to your passwords, what a vault is to a bank. It's simply a secure vault for storing passwords. It's like outsourcing the remembrance of your passwords to an app, installed on your laptop, smart phone or any other computing device.

### Why You Need a Password Manager



Your brain has better things to do than store several unique passwords.

They're excellent at preventing password re-use. With so many accounts to keep track of, the temptation to reuse the same password is understandable.

Sure, you may alter it slightly by adding a different number at the end or throwing in an exclamation point.



## Activities

But while this may seem like a solid plan for remembering passwords, it also leaves you vulnerable to password reuse attacks. A password reuse attack occurs when a hacker gets their hands on the password for one hacked account, then tries using it to sign-in to other websites.



Your passwords are too simple. If you're using passwords that you can easily remember because of how simple they are, you are at risk.



Password managers include random password generators, to help you create complicated passwords.



You only need to remember one password. With a password manager, you only need to remember one password – the one used to gain access to your stored passwords.



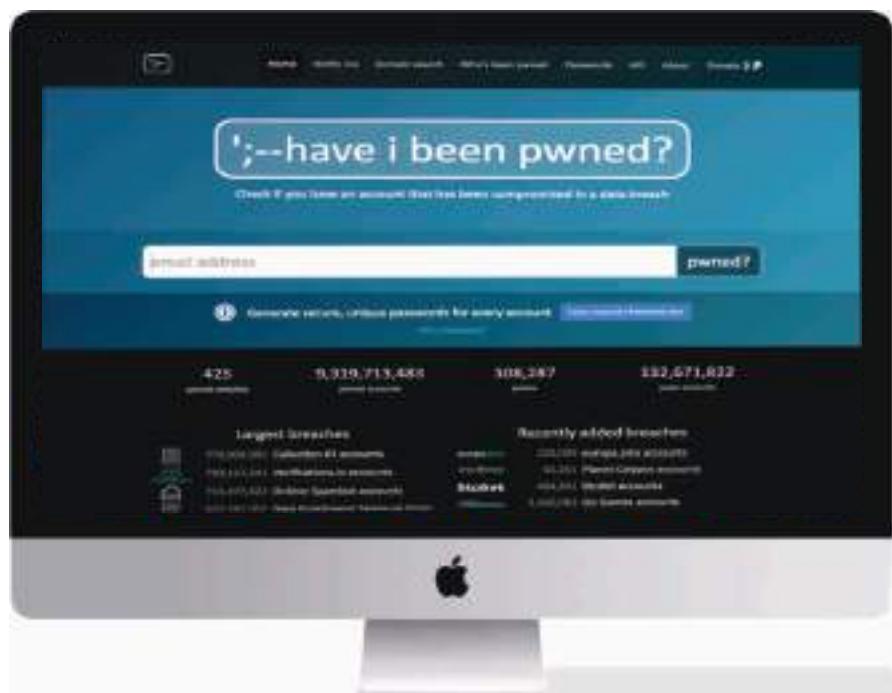
The numbers are against you. How many accounts do you have that require passwords? Given that you must use different passwords for every account, how many secure passwords can you memorize anyway?



Sync your passwords across devices and have them handy for when you need them. Some password managers can help you autofill your login information when you request it to do so.

**ACTIVITY 5:**

check if you  
have an account that  
has been compromised  
in a data breach



Visit  
[www.haveibeenpwned.com](http://www.haveibeenpwned.com)  
and search across multiple data  
breaches to see if your  
email address has been  
compromised in the past

## Activities



#NoGoFallMaga is a national movement of young people, working to combat preventable incidents of cyber fraud in Nigeria, with consumer-centered sensitization and education. Cyber fraud in this context includes email deception and phone-based scams, particularly where cybercriminals impersonate trusted organizations. We leverage on fun experiences and content, to catalyse the decline of cyber-related fraud, one trickle of knowledge and advice at a time.

We believe that until fraud becomes unprofitable, it will continue to run as an undesirable parallel economy and hence remain attractive to Nigerian youths. The #NoGoFallMaga campaign is dedicated to raising awareness on digital fraud issues, in order to equip Nigerians with cybersecurity knowledge for better decision making and fraud mitigation.

From the middle-aged women in the market, to the white collar executives, to the young men in university campuses and even to the seniors across Nigeria; no individual with access to financial services and technology will be unreached with our message.

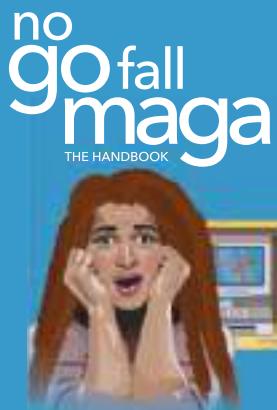
#NoGoFallMaga is an initiative of CyberSafe Foundation and for more information, please visit [www.nogofallmaga.org](http://www.nogofallmaga.org)



In an age in which everyone has a phone and is online, it is not at all surprising that we have all become highly-sought-after targets of criminals and criminal activity, lured by the immense value in all those devices and online identities. Far too many people have fallen victim, and many more will, sadly, in the future. That's why the 'No Go Fall Maga' handbook is a timely and necessary intervention, to protect and secure multitudes of vulnerable consumers. It is, literally, a lifesaver. While reading it I paused to immediately enable two-tier authentication on my WhatsApp account. That's just one evidence of how immensely practical and helpful – and timely – it is.

**Tolu Ogunlesi**

Special Assistant to the President of Nigeria on Digital and New Media.



"Security begins with the human behind the technology; Sometimes the solution to that somewhat technical situation is not as technical as we imagine. This book breaks down seemingly complex issues and makes it relatable to the everyday human. The stories, puzzles and activities makes application of the lessons easy. After reading this book, the regular digital citizen will be armed with the right information to keep themselves and organization safe from the evil that's lurks around the internet."

**Elizabeth Wuraola Kolade**

Cyber Security Professional

#NoGoFallMaga addresses the issue of Cybersecurity through real-life experiences and what should have been done. It is simple to read and interesting. This is a must-read for anyone wanting to understand the basic issues of cybersecurity.

**Dr. Babatunde Oghenobruche Obirimah**

Chief Operating Officer, Fintech Association of Nigeria.

#NoGoFallMaga's Cybersecurity Awareness Handbook is an easy to understand guide to becoming more cyber-security conscious.

This well-written handbook wins by using relatable stories with clear indicators of errors and the correct actions to be taken, showing the reader how to easily incorporate simple but essential safety tips into daily life and interactions in our increasingly technology-dependent world.

**Arit Okpo**

Host, CNN African Voices

