NoGo FallMaga

Powered by: cybersafe. FOUNDATION

Cybersecurity Awareness Month with NoGoFallMaga

CYBERSAFETY FOR SENIORS: **PROTECTING THE ELDERLY FROM FINANCIAL EXPLOITATION**

FRIDAY 16TH OCT. 2020

6.00PM

Free Registration:
bit.ly/NGFM-CSAM2

Speaker:
Samaila Atsen Bako
Director, Social Media and Communications CSEAN

#NoGoFallMaga

CYBERSAFETY FOR SENIORS

Protecting the Elderly from
Financial Exploitation

SAMAILA ATSEN BAKO

Our Reality

- As of June 2019, figures from Statista showed that Nigeria had 123.49 million internet users. Out of this figure, 74 percent of web traffic was generated via smartphones, and only 24 percent via PC devices.

- More devices = More users = More Victims ?

Key Questions

- Why are you a target?
- Why are online scams so rampant?
- What are some examples?
- How can you spot them?
- How should you respond to them?

A freedom of information (FOI) request submitted by the charity to Action Fraud, showed that the police received 4173 reports of cybercrime from people aged 55+ from April 2018 to March 2019. Of those that became victims, a total loss of just over £4m was recorded. Those in this age group represented 19% of the overall number of reported cybercrime victims in this period.

Why You?

- Data is the new oil
- Identity theft or impersonation
- Business Executives & VIPs
- Retirement benefits
- Next of Kin or Inheritance
- More likely to be:
  - Less tech-savvy
  - More trusting
  - Lonely

Why So Rampant?

- The internet is powerful
  - Free tools
  - Free tutorials
  - Anonymity of attackers
- Social media provides all the necessary personal information
  - LinkedIn profile
  - Press releases, articles and blog posts
  - Children's Instagram posts, Tweets, and so on

Financial Fraud

A Closer Look at Some Common Scams

SMS Scams

- Also called SMiShing

- Hooray!!! You have just won N2 million. Call this number NOW to redeem our reward.
- Congratulations. You have been selected to receive an iPhone11. Call John now on … to verify your identity and receive your gift.

Phone Call Scams

- Also called Vishing – voice solicitation

- Common scenarios are:
  - Child is involved in an accident
  - Nephew has been arrested by SARS
  - Grandchild has been kidnapped
  - Pastor Joshua gave me your number…
  - Bank customer service
  - Company representative (HR, Finance, IT support)

ATM Skimmers

Email Attacks

- Email Scams – Phishing
- Email Compromise
- Malicious links and attachments
- Spamming – Unsolicited Bulk/Commercial email

Email Scams - Phishing

- Billions of email accounts exist
- Emails are easily sent out instantly

Fwd: Inbox

Benjamin Gmatchame 10:38 AM

to bcc: me

Hi;
I am Erich Jonathan, the solicitor of a late client who died of kidney cancer with an unidentified family
or relative. I am contacting you to stand in as a next
of kin to his deposit of (Five million eighty-sixty thousand dollars), Thank you for your understanding.
Please reply as soon as possible for more information.
Regards,

Mail Delivery Subsystem 11:46 AM

to me

Address not found

Your message wasn't delivered to **gmatchameb@gmail.com** because the address couldn't be found or is unable to receive email.

LEARN MORE

The response was:

```
550 5.2.1 The email account that you tried
to reach is disabled. Learn more at
https://support.google.com/mail/?p=DisabledUser
q186sor273335oif.158 - gsmtp
```

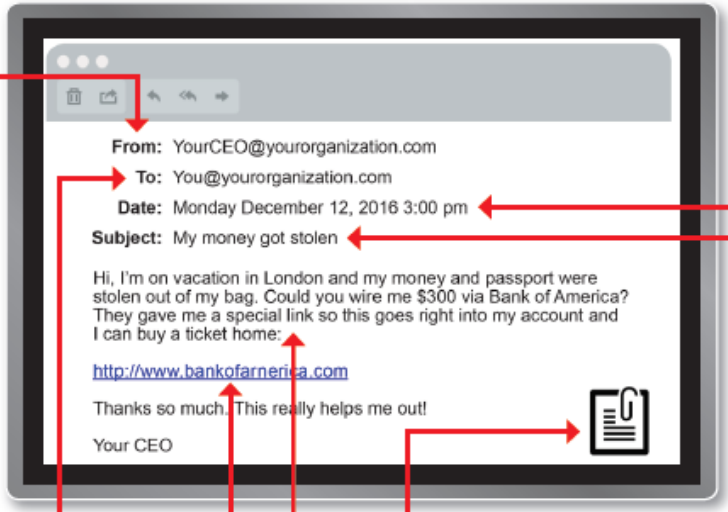
What to Look out For

- Too many scams, but here are the red flags:
  - Too good to be true (a get rich quick offer)
  - Out of the blue or unexpected
  - Requires you to provide personal & financial information
  - Requires urgent action
  - Generic salutation like “Dear Customer” or “Hi”

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Reminder: update required due to payment issue

March 3, 2020 7:41 PM

Netflix Inc

Details

Spotify

Dear **Customer**,

We recently added a new security verification for All Spotify account

We require from our Costumers to check and update their account information.

You will not be able to use your Spotify Account until this proce is complete.

Please click on the link below to proceed:

https://open.spotify.com

Sincerely,

Please do not hesitate to contact us, if you have any inquiries.

Thank you .

NETFLIX

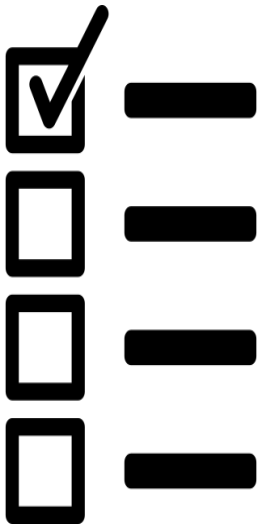
Dear Valued Customer,

We're having some troubles with your current billing informations.

We'll try again but in the meantime you may want to update your payment details.

Update now >

Your friends at Netflix.



Can you tell the difference between legitimate & phishing websites?

https://www.opendns.com/phishing-quiz/

Email Compromise

- Typical causes:
  - Weak passwords (common, short, simple)
  - Repeated passwords
  - Seldom changed passwords
  - No 2-Factor Authentication
  - Shared passwords
  - Written passwords
  - Unlocked devices
  - Sharing habit online

Malicious Links & Attachments

- Malware can be downloaded to steal information or silently conduct surveillance
- Links can be used to collect certain information or even compromise your system

Social Media Attacks

Cyber Attacks Perpetrated

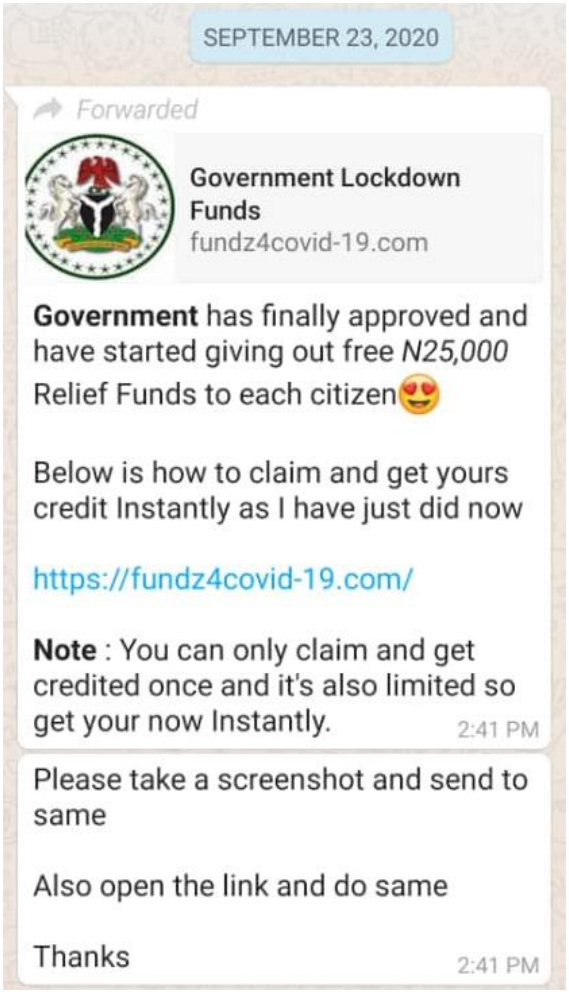
via Social Media

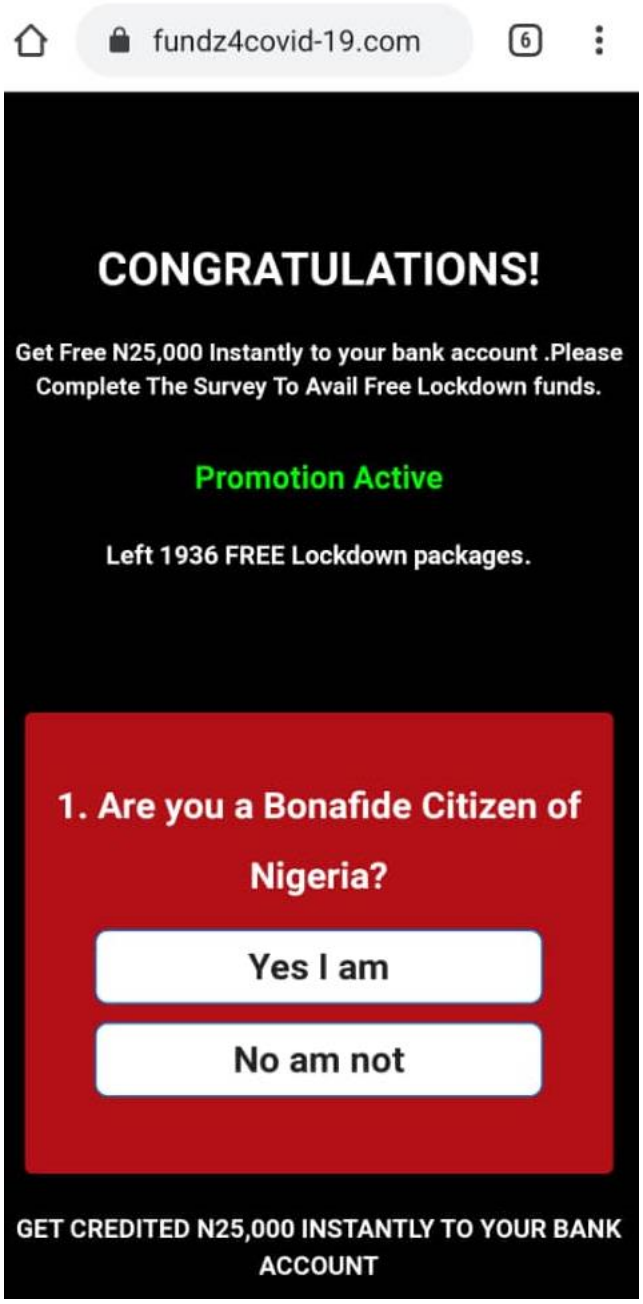
WhatsApp Hijack

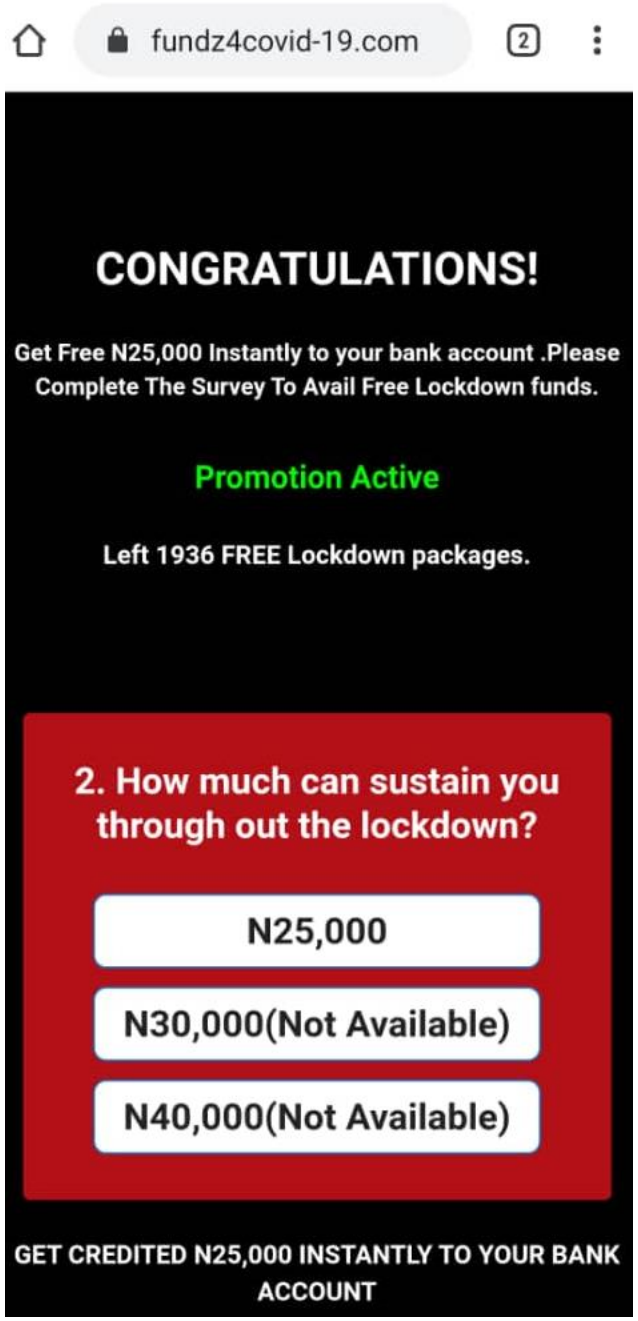
- Relatively easily to execute
  - Stolen phones
  - Sim swap
  - Malicious app or update
- Very attractive
  - Reach - Forwarding to groups and individuals
  - Trusted identity
  - Valuable data
  - Ease
  - Guard is down

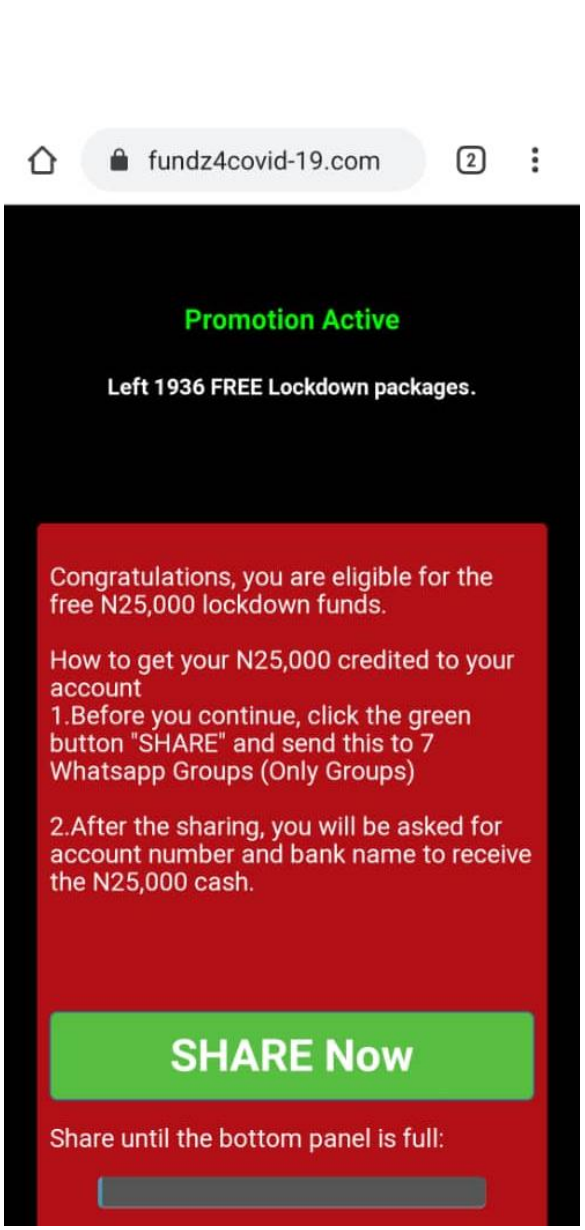
WhatsApp Scams

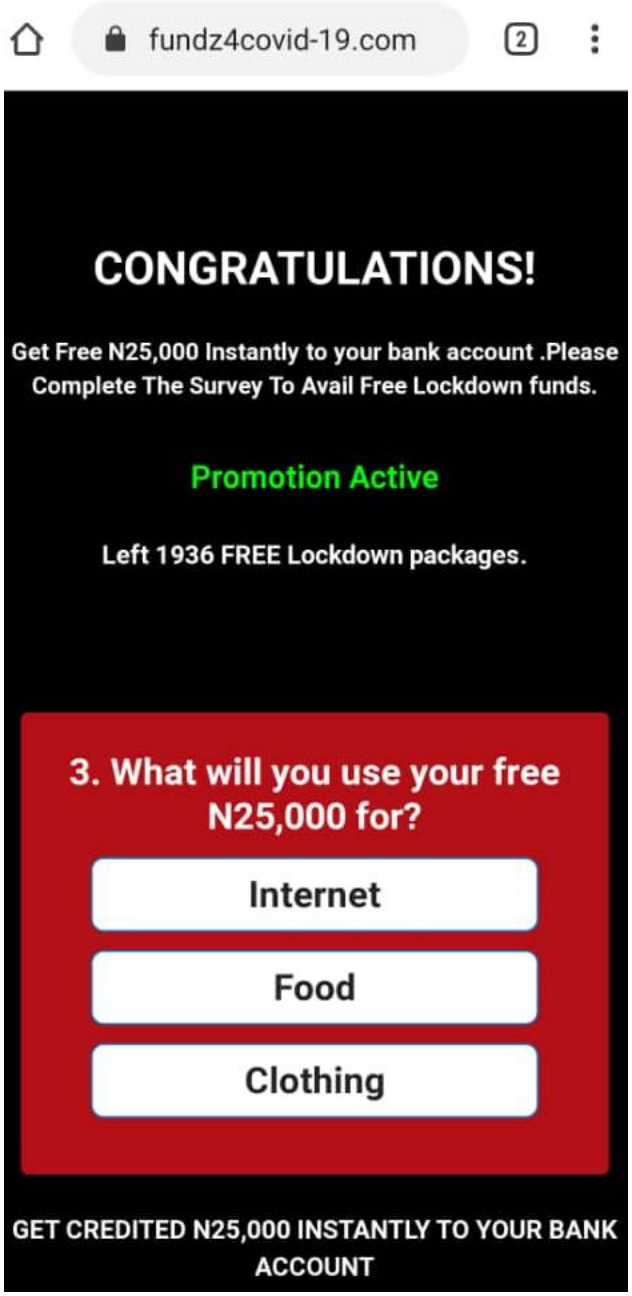
- Malicious links forwarded to individuals and groups
- False information widely distributed
- No way to verify actual source of information
- Fake business accounts
- Request for urgent help
- Request for information


SEPTEMBER 23, 2020
Forwarded
Government Lockdown Funds
fundz4covid-19.com
Government has finally approved and have started giving out free N25,000 Relief Funds to each citizen😍
Below is how to claim and get yours credit Instantly as I have just did now
https://fundz4covid-19.com/
Note : You can only claim and get credited once and it's also limited so get your now Instantly.
2:41 PM
Please take a screenshot and send to same
Also open the link and do same
Thanks
2:41 PM


fundz4covid-19.com
6
CONGRATULATIONS!
Get Free N25,000 Instantly to your bank account .Please Complete The Survey To Avail Free Lockdown funds.
Promotion Active
Left 1936 FREE Lockdown packages.
1. Are you a Bonafide Citizen of Nigeria?
Yes I am
No am not
GET CREDITED N25,000 INSTANTLY TO YOUR BANK ACCOUNT


fundz4covid-19.com
2
CONGRATULATIONS!
Get Free N25,000 Instantly to your bank account .Please Complete The Survey To Avail Free Lockdown funds.
Promotion Active
Left 1936 FREE Lockdown packages.
2. How much can sustain you through out the lockdown?
N25,000
N30,000(Not Available)
N40,000(Not Available)
GET CREDITED N25,000 INSTANTLY TO YOUR BANK ACCOUNT


fundz4covid-19.com
Promotion Active
Left 1936 FREE Lockdown packages.
Congratulations, you are eligible for the free N25,000 lockdown funds.
How to get your N25,000 credited to your account
1.Before you continue, click the green button "SHARE" and send this to 7 Whatsapp Groups (Only Groups)
2.After the sharing, you will be asked for account number and bank name to receive the N25,000 cash.
SHARE Now
Share until the bottom panel is full:


fundz4covid-19.com
CONGRATULATIONS!
Get Free N25,000 Instantly to your bank account .Please Complete The Survey To Avail Free Lockdown funds.
Promotion Active
Left 1936 FREE Lockdown packages.
3. What will you use your free N25,000 for?
Internet
Food
Clothing
GET CREDITED N25,000 INSTANTLY TO YOUR BANK ACCOUNT


GET CREDITED N25,000 INSTANTLY TO YOUR BANK ACCOUNT
Like · Share · Comment · Remove
others 204,208 like this
more comments... 63 of 173,330
Khomotso Polivia
Thanks for this lockdown gift!! I got N25,000 for free just now
Just now · Like
Bokang Mosala
First i Thought it was Fake,But Really Credited
Just now · Like
Rakumako Shoki
Wow I've been credited just now.. Thank you
Just now · Like
Thato Maria
Thank you !
Just now · Like
Ntuli Kgosana
I have received mine and my friends must also be aware of this!!!
Just now · Like
Tebogo Ratime
Fantastic! Thank you a lot for this
2 min ago · Like 223
This offer is limited only till 25th of October .. Hurry!! So far 108544 users have received their N25,000 Lockdown funds.

WhatsApp Recovery

How to recover your account

Sign into WhatsApp with your phone number and verify your phone number by entering the 6-digit code you receive via SMS. Learn more about verifying your phone number in our Help Center: Android | iPhone.

Once you enter the 6-digit SMS code, the individual using your account is automatically logged out.

You might also be asked to provide a two-step verification code. If you don't know this code, the individual using your account might have enabled two-step verification. You must wait 7 days before you can sign in without the two-step verification code. Regardless of whether you know this verification code, the other individual was logged out of your account once you entered the 6-digit SMS code. Learn more about two-step verification in this article.

Note

- If you have access to your account and suspect someone is using your account via WhatsApp Web/Desktop, we recommend to log out of all computers from your phone.
- To protect your account, WhatsApp will notify you when someone tries to register a WhatsApp account with your phone number. Learn more in this article.

https://faq.whatsapp.com/general/account-and-profile/stolen-accounts/

Account Hijack/Takeover

- Malicious links sent via different social media platforms to unsuspecting victims from a hijacked account
- Spread of false/misleading information
- Fake businesses
  - Investment opportunities
  - Anti-ageing creams or drugs
  - Libido boosters E.g.: Viagra

BREAKING: Major Twitter accounts, including Elon Musk, Bill Gates, Uber, Apple and more, appear to be compromised by bitcoin scammers.

Suspected bitcoin scammers take over Twitter accounts of Bill Gates, Elon Musk
nbcnews.com

Mike Bloomberg @MikeBloom... · 9m
I am giving back to the community.

All **Bitcoin** sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

398 815 707

Joe Biden @JoeBiden · 38s
I am giving back to the community.

All **Bitcoin** sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

72 72 102

Romance Scam

- Aim is usually financial gain
- Promise of love and attention
- Typically requires some money to buy flight tickets or sort out some issue or the other
- Friendship and trust is built over time before exploiting the victim
- Not too common locally, but your friends and family abroad may need this information

Romance Scam

General Security Tips

How to Guard Against Cyber Threats

What Can You Do?

- Use strong passwords (long, private, uncommon)
- Use 2-Factor Authentication
- Always update apps & firmware promptly
- Use only official app stores
- Lock sim cards and devices

What Can You Do?

- Trust but Verify
- Use official contact information from authentic websites or social media handles
- Stop.Think.Connect
- Seek professional opinion or help
- Report anything suspicious

What Can You Do?

- Make your accounts private
- Delete unused/old accounts

- Share with care
  - Home, school & work addresses
  - Banking information (BVN, bank, account number)
  - Card information (number, cvv2, pin, expiry date)
  - Travel information (date, time, airline, destination)
- If you must share, do not do it in real-time

Password Managers

- Why?
  - Generate strong passwords
  - Safe storage
  - Available across devices
  - Multiple users (shared accounts)
  - Autofill (risky)

- Examples: LastPass, 1Password, NordPass etc.

Creating Strong Passwords

- Use a Phrase (3+ words)
- Use different types of characters
- Make it long (8+ characters)
- Examples:
  - H0neyI'mHom3%
  - tru5tBUTv3r!fy
  - aWo0fd&bel!3
  - h3avenIMh0me*
  - CySecIAShar3d&

www.howsecureismypassword.net

Toothbrush = Password

- Pick a good strong one
- Do not share with anyone
- Change it regularly
- Do not reuse an old one
- Supplement with floss & mouthwash (2FA)

- Go ahead and change that 3-year old password NOW!!!

Q&A

Thanks for listening!!!

Do me a favour and connect with @stcnaija & @cyberexpertsng on Twitter and Instagram

SAMAILA ATSEN BAKO

@atsen_ Linkedin.com/in/atsenbako

NoGo FallMaga