shineyoureye

Sabi

The Toolkit

Powered by cybersafe. FOUNDATION

Social Media Protection

What is 2- Factor Authentication A.K.A 2FA?

"Is this really you?" is the question Two-Factor Authentication asks whenever you want to log in to your online accounts.

Two-Factor Authentication provides an extra layer of security and doesn't give you access just because the username and the password are correct; but demands another code when you try to log in. This code could be sent to your phone via text message, email or generated by an app on your phone (an authenticator app) depending on your setting.

Just like the burglar proof on windows and doors that stands between thieves and your valuable items, 2FA stands between your online accounts and cybercriminals (fraudsters)

Reasons To Set Up 2FA

- It is free and easy to set up
- It provides an extra layer of security even when your login details (password) have been stolen.
- Protects you from data loss and identity theft.
- It makes it harder for fraudsters to steal from you.

Three Things You Need To Set up 2FA

Have you ever heard of an Authenticator app?

It's an app that helps you complete your two-factor authentication process by generating passcodes. The app isn't connected to your phone number so it's one of the topmost and highly recommended way to go about activating 2FA. An example of an Authenticator app is the Google Authenticator (available on play store and iOS App Store)

Let me guide you through turning on Two factor authentication on a WhatsApp and Facebook.

P.S You can activate two factor authentication on all social media accounts and mobile banking apps.

You can set up 2FA everywhere.

WhatsApp

- Open the WhatsApp app on your phone
- Tap the three dots in the upper-right corner
- Tap **Settings**
- Tap **Account**
- Tap **Two-step verification**
- Tap **Enable**
- Enter your custom PIN
- Re-enter your custom Pin
- Tap **Next**
- Enter your email address
- Re-enter your email address
- Tap **Save**
- Tap **Done**

Facebook

- Login into your Facebook account
- Go to settings and privacy
- Click on settings
- Scroll down and click on Security and login
- Click on use two-factor authentication
- Choose Text message (SMS) and click continue
- Enter your phone number and click confirm
- Enter your password to confirm it is you
- Enter the code sent to you
- You will then see a confirmation screen

What To Do When You Lose Your Phone

The loss of a mobile phone can result in a huge discomfort what will make it worse is if the loss of your phone causes you to lose your hard-earned money. Wondering how this is possible? Mobile banking.
Almost everyone makes use of the mobile banking service, using USSD (short code) or mobile app to perform bank transactions on their phones.

USSD A.K.A quick code is communication method used by customers to communicate with their network service providers or for mobile financial services. When you dial a number that starts with * and ends with #, you are using USSD.

There are two actions you must take to prevent loss of funds when your phone gets stolen,
1.Lock your SIM card; this should be done before the phone is missing)
2.Block your bank account; this should be done immediately you discover the phone is missing.

How To Lock Your SIM Card

iOS Device

- Go to Settings on your iOS device.
- Tap on Mobile Data.
- Locate SIM PIN and tap it.
- Toggle the SIM PIN to ON.
- Input your current SIM PIN if the SIM wasn't locked use the default pin below
- Click on Change PIN
- Input the default PIN again
- Enter a new SIM PIN to lock your SIM card
- Press Done
- Make sure that you remember it!

Android Device

- Go to settings, then Security.
- If you are using a dual SIM phone, select the SIM card you want to lock.
- Set up SIM card lock.
- Enter the default SIM PIN.
- Tap Change SIM PIN.
- Enter old SIM PIN and press OK.
- Enter new SIM PIN to lock SIM card.
- Confirm the new four-digit PIN.
- Press OK and exit.

The default pin for
MTN = 00000, Airtel = 1234, Glo = 0000 and 9mobile = 0000

How To Block Your Bank Account

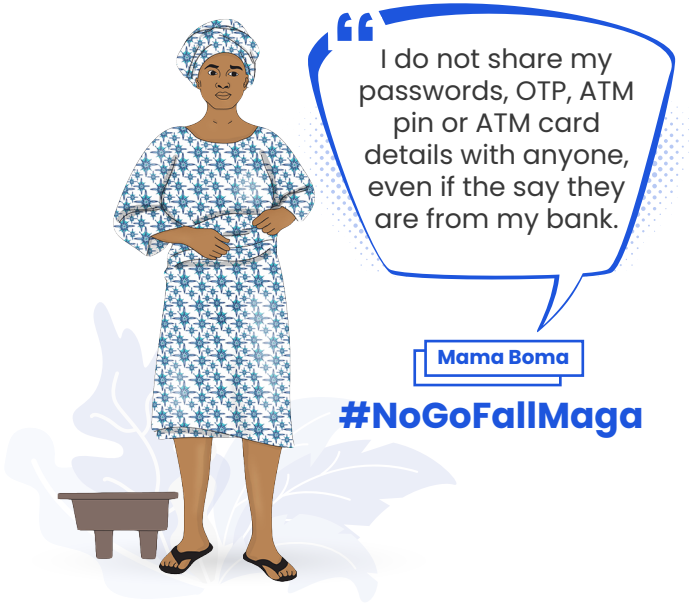
Bank	Action
Access Bank	Dial *901*911# from any phone or call +23412802500
EcoBank	Dial *326*911*1*phone number# from any phone or call 0700 500 0000
Fidelity Bank	Dial *770*Phone number # from any phone
First Bank	Call 07080625000 from any phone
First City Monument Bank	Dial *329*911# from any phone or call 0700 329 0000
Guarantee Trust Bank	Dial *737*51*74# from any phone
Heritage Bank	Dial *745# and follow the instructions
Keystone Bank	Dial *7111*911# from any phone or call 23470020003000
Polaris Bank	Call 08069880000 from any phone
Stanbic IBTC	Call 01-422-2222 from any phone
Standard Chartered Bank	Dial *977*991# from any phone or call 012704611 from any phone
Sterling Bank	Dial *822*911# from any phone or call 0700 7837 5464
United Bank of Africa (UBA)	Dial *919*9# from any phone or call 0700 225 5822
Union Bank	Dial *826*6*Phone Number# from any phone
Unity Bank	Dial *7799*9*Phone number# from any phone
Wema Bank	Dial *945*911# from any phone
Zenith Bank	Dial *966*911# from any phone

Abbreviations You Must Know

CVV
The three-digit number written on your ATM card

OTP (One Time Password)
An automatically generated code sent by a service provider that is used for a single authentication process. It is usually 6 digits and is often received via SMS.

BVN (Bank Verification Number)
An 11-digit number used to uniquely verify the identity of each bank customer across all financial institutions.



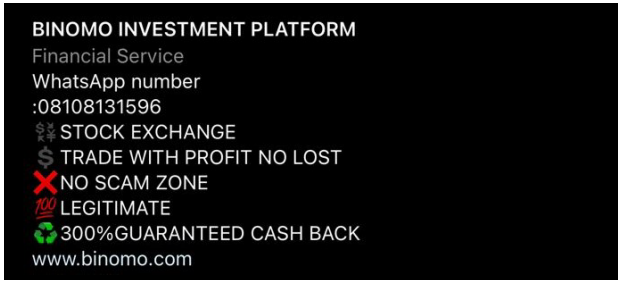
INVESTMENT SCAMS

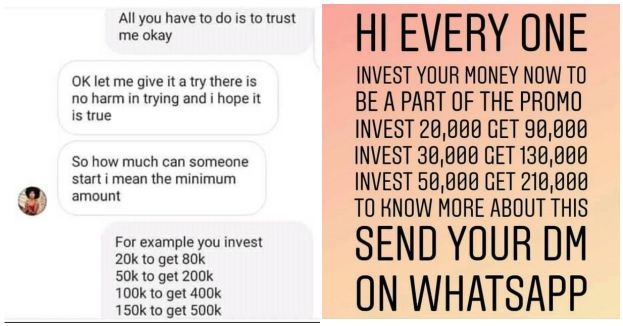
Fraudsters often hide behind fake investments schemes to trick unsuspecting individuals and take away their money. While this continues to be a growing trend, we must find a way to protect ourselves while looking for ways to grow our income.

Red Flags of Investment Fraud

- It promises high profit and low risk.
- The investment has a short lifespan (Invest 50,000 and get 300,000 in 2 weeks)
- Its core message is “everyone is doing it and it is paying”
- There is pressure to invest immediately.
- They are not registered to sell investments.

Examples of Investment Fraud





How To Protect Yourself from Investment Scams

- Verify credentials. Do not fall for a fancy title or other appearances of success, ensure they are properly registered.
- Do not chase "quick riches." Be sceptical of investment pitches that guarantee a certain return or promise spectacular profits.
- Be wary of a sales pitch that focuses on how many people are investing, without telling you why the investment is sound. Do not believe claims that "everyone" is investing in the scheme.
- Be suspicious of investment opportunities that promise a high return with little or no risk.
- Refuse to be rushed. If the salesperson tells you that the offer is for a limited time only, or that investment opportunities are limited, consider it a red flag. A legitimate investment will still be there tomorrow.
- If you feel an offer to buy shares might be legitimate, always check the company's listing on the stock exchange for its current value and recent shares performance. Some offers to buy your shares may be well below market value.
- Do not give your details to an unsolicited caller or reply to emails offering financial advice or investment opportunities - just hang up or delete the email.
- Never commit to any investment at a seminar - always take time to consider the opportunity and seek financial advice from a more knowledgeable person.
- Never feel obligated to invest because the seller gives you something for free.
- Arm yourself with information. Learn to spot the red flags of investment fraud so you can protect yourself and your loved ones.