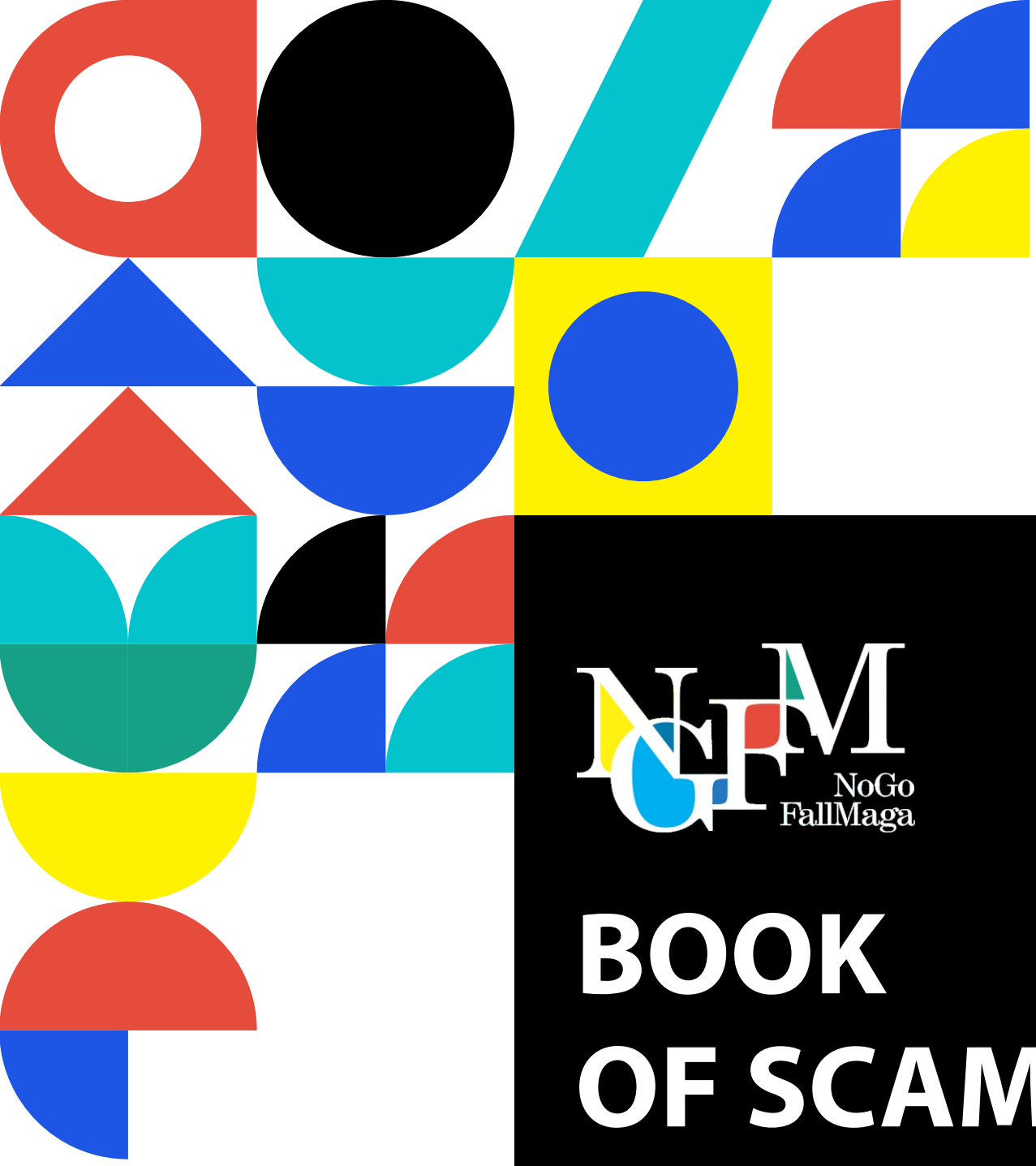


NoGo FallMaga

BOOK OF SCAMS

cybersafe. FOUNDATION | tell two

www.nogofallmaga.org

Table of Content

Introduction

Every year, Nigerians lose billions to diverse types of scams. These scammers use a variety of means to target their victims, from face-to-face interactions to electronic communication. Scammers are relentless and keep improving their methods. This booklet is a response to this situation. It covers the most prevalent scams in our country and offers practical steps you can take to protect yourself. We hope that this booklet will help prevent you from being a victim of the despicable activities of scammers. We also ask that you share this information with family and friends, for this is a sure means to make sure that they are also protected.

A quick word.... Research and think, before you leap.

Scammers are successful because they are students of human nature and adept at manipulation. One of their major ploys is to evoke strong emotions in their victims that short circuit the ability to think. Hence, a lot of scams can be avoided by pausing to think and refraining from taking action. Also, since thinking does not occur in a vacuum and needs the relevant information, doing the necessary research or getting someone to do it for you, is an aid to proper thinking and apprisal. We can't say this enough, before you hand over your money or sensitive information, make sure you have done adequate research and thought hard about the step you are about to take. Finally, as the saying goes, two heads are better than one. Always seek counsel from industry professionals or other more knowledgeable than youself, this serves as a failsafe in case you miss something.

Charity Scams

Most humans want to do good for a plethora of reasons. Some do it for philanthropic reasons while others for reasons best known to them. But whatever their reasons may be, this automatically makes them potential targets of 'Charity scams'

Charity scams are schemes devised to deprive unsuspecting people of their funds by preying on their generosity. This can take many forms but mostly through scammers pretending to be legitimate charities. In such instances, they ask for funds pretending to be victims of a recent disaster, veterans from the military, orphanages, or people with serious medical conditions.

Charity scammers use every available means to approach their victims, they can approach in person, via e-mail, telephone, SMS, and social messaging applications. They use logos and images of real charities and victims or create fakes using image editing applications like photoshop. Unfortunately, most charity scams go unreported because the victims committed sums they consider expendable. This sustained precedence encourages its occurrence.

Here are some ways to figure out if that call, e-mail, SMS, social media post/message or pitch is legit.

- **Fake Charities are not registered.** A reputable charity organization should be registered with the government. To know if a charity is registered, you can look them up from the **CAC name search portal**, the portal gives details about an organization's registration date, branch address, and contact information.

- **They use pressure and urgency.** Reputable and legitimate Charities do not pressure people into donating no matter how urgent a situation may be. In contrast, scammers treat 'donations' as a matter of urgency, pressuring you into making donations. They employ emotional blackmail, aggressively pushing victims' stories with the aim of manipulating the donors.

- **They accept donations through channels that aid anonymity.** Given the unprecedented proliferation of payment technologies, scammers now employ alternative channels of payment, especially those that protect the identity of the receivers. These may include Cryptocurrencies, Gift Cards, and Wire Transfers that are untraceable, so you should watch out for this. Legitimate charity organizations will always accept a variety of payments methods including traditional methods that supply an audit trail.

- **They spam you with messages.** Fake charities spam people with messages or links for donation. Legitimate charities do not do this, instead they usually have a webpage with clear information on how to donate and where.

Steps for protection

- **Verify their "good works"** Don't be swayed by responses such as "we take care of the needy" or "we support widows and orphans," without actions these are empty words. Seek out concrete proof that they engage in the work they claim with verifiable results. For instance, if they claim to take care of orphans, find out where their orphanage is, how long they've been involved in the work and the difference it has made in the lives of the children.

- **Do some checks on their website.** Scammers can clone a charity organization's website and content. They then slightly alter the domain name (For example, www.nogofallmaga.org can be misspelled as www.nogofalmaga.org). How can you be vigilant and not fall for this? You can do so by using these online tools to check if a website is a clone and if the content of the website is used elsewhere; **CopyScape, SiteLiner, PlaqSpotter**. You can also make use of **reverse image search** to check if images on the website are being used on other sites.

- **Verify Crowdsourced or social media appeals:** Before you give out money for a GoFundMe or social media appeal for aid, make sure you can verify the situation is true or that you personally know the person asking for funds. If you can't then you should consider not giving no matter how tragic the situation is portrayed to be.

- **Approach the charity yourself.** Always physically check out the charity organizations you are willing to donate or offer support. Do not rely only on a phone number, contact or website address given by the person who first called, visited, or emailed you because they could be impersonating a legitimate charity.

REMEMBER

- If you have any doubts about the individual or organization asking for money, do not proceed.

CAUTION

- Never give out personal information over the phone or through SMS and verify the authenticity of the charity's website before entering your card details to make a donation.

THINK

- Why are they pressuring me to give money, are they really genuine?

Romance Scams

The advent of the internet brought about a new phenomenon called online dating, which is romantic relationships via the internet, traditionally on dating sites, now extended to forums and social messaging applications.

Unfortunately, not everyone using the internet for online dating is looking for love. Scammers use fake profiles and identities to befriend people on social platforms. Scammers know people are looking for romantic or committed relationships, and their aim is to manipulate such people for monetary benefits.

Are you at risk?
While some romance scammers may work like spammers, casting as wide a net as possible, others are more clinical and select their victims. They seek targets that are more open to their manipulation, such as those who have recently experienced heartbreak, divorce, or loneliness. Also, those fond of sharing information on social media about personal issues and matters of the heart are targets for romance scammers.

Warning Signs

Grammar: Compare a person's grammar to their background. For instance, someone who claims to be well educated but keeps making grammatical blunders should sound the alarm bells as scammers are not well-educated.
Also, if a love interest sends a message or email, copy, and paste parts of it in a search engine to see if it has been used elsewhere on the internet. If it has, that is a warning sign because scammers often use the same format of messages on different targets or copy stuff straight off the internet.

Change of platform: Beware of immediate requests for change of communication channel. You meet someone on a dating app, and the person at once asks you to continue the chat via WhatsApp or some other platform.

Asking for money: Scammers usually ask for gift cards, recharge cards, subscription payments, or that a family member is in the hospital and cash is needed.

Love bombing: Someone you just met has already started bombarding you with love messages. Scammers are known for trying to get intimate with their victims at once.

Scanty social media: You check out their social media account and see a few photos, few posts, few friends, and the connections they have are of the same sex.
Avoids meeting physically: Something always comes up when you have to meet physically, giving excuses as they're traveling, have an emergency, family problems, or a business deal went sour.

Steps for Protection

Go slow. Take it slowly. Ask your potential suitor lots of questions and gauge their answers. Watch

out for inconsistencies that might point to the fact that you're dealing with a scammer.

Never Send Photos. Do not send photos, especially those taken nude or in compromising positions. These could be used for extortion.

Do not receive money. Do not agree to receive or transfer money. Romance scammers are often into other forms of cybercrime and are constantly on the lookout for those to use to launder money.

Do a photo search. Always perform a reverse image search. The means downloading the person's photo and doing a "search by image" on Google, Bing, and Yandex to see if the person's photo shows up on other places under a different name.

Don't give out personal details. Till you are sure you're not being scammed it is better not to give out personal details. Requests for a phone number, address, work details should be met with the response "I don't give out my personal details till I know someone better and meet them in person."

Verify details. Do a Google search of every single detail from your potential love interest. Start with their names, address, or any other details they give to you. Check for inconsistencies with their chats or claims.

REMEMBER

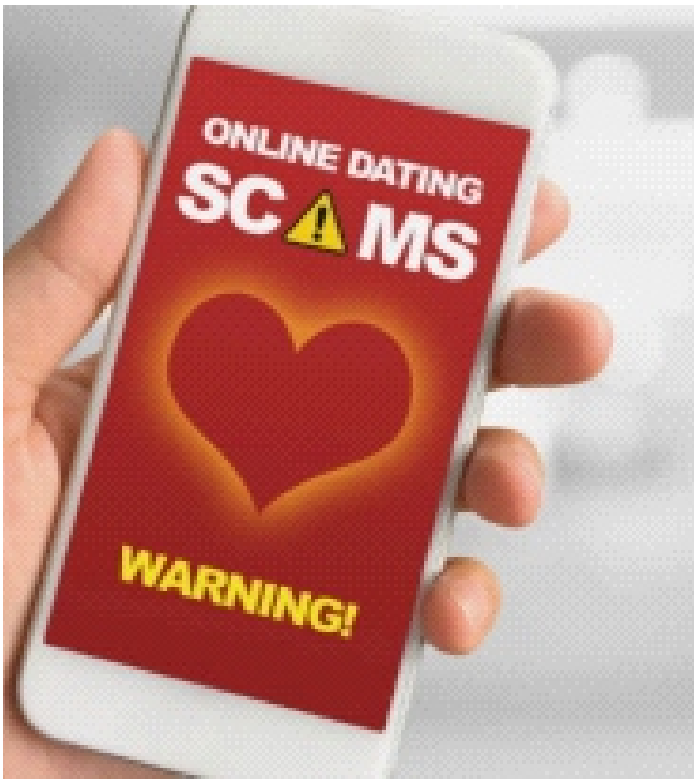
- Not all profiles on dating sites are real.

CAUTION

- Be wary if your online interest quickly professes love.

THINK

- This is someone I haven't met in person, should I be sending money?



Emergency Scams

Emergency scams, as the name implies, are scams that present a situation in which a friend or family member is in dire need of help. Scammers can use all sorts of pretexts, from accidents to arrests, with the aim of presenting a plausible scenario where they can extract money. A typical emergency scam begins with the scammer collating information about the target, through social media or some other means. When satisfied, the scammer would then go ahead to devise a pretext. For instance, they could claim to be an administrator of a boarding school and contact a parent whose child is enrolled in that school, informing them that their ward has been involved in an accident. Or they could pose as the chairperson of a Local government association that is abroad and inform a family member that their relation has been arrested in that foreign country and needs help. In such scenarios the scammer would supply convincing details such as family names or school details and the pretext chosen would depend on the information gotten on the target.

Also, scammers employ the following tactics to aid the success of the scam

- Getting an accomplice to impersonate an authority figure. This makes them sound more convincing and scares the target.
- Asking the target to act quickly and not bother informing others to save time

Steps for Protection

- Be careful of what you share online and on social media. Also, check what family members share online so you have knowledge of how much of their personal information is available online.
- Do not act at once. End the call and find some other means to verify the information, either through another family member or an acquaintance.
- Ask a very personal question, the type you know will be difficult for an imposter to answer.

REMEMBER

- Resist the urge to act quickly no matter what you're told.

CAUTION

- Never send money to someone you don't know.

THINK

- Is there a friend or family member I can ask for confirmation?

Juju Scams

Juju scams are scams that prey on the belief that non-material entities (Deities, Spirits of Ancestors, Angels/Demons) can affect or change the normal events of life, especially with regards to supplying financial help, improving luck, or mitigating adverse circumstances.

Juju scammers often set up operations in a remote village or town where they open a shrine. One of them takes up the role of a "priest" or "babalawo" while the rest fish for targets using both physical and virtual means. Virtual tactics range from making claims on social media and social messaging apps about having powers to confer wealth or solve diverse problems to sending threatening text messages about doom and how the recipient needs to come for a consultation to avert the impending disaster. As always, these scammers are refining their tactics but the working principle in these types of scams is their alleged power to alter the current situation to the benefit of their target.

In some cases, to prevent detection, they demand their prospective victims not to show these interactions with friends or family as this might interfere with the efficacy of the charms or incur the wrath of the deity leading to death. Also, some of these scammers are skilled at illusions and the sleight of hand tricks, coupled with the help of accomplices giving false testimonies, this makes their racket look very convincing.

The end game is always about money, as victims will be asked to buy items for spiritual cleansing or to bring certain amounts to ward off disaster or induce good fortune.

Steps for Protection

- Be wary of testimonies about solutions to problems or wealth after visiting a shrine
- Do not visit shrines for healing, wealth, or remediation of problems
- Disregard communications via text messages or messaging apps about prophecy, dreams, visions, or divinations about you, do not respond
- Do not share personal information on social media or the internet, most especially about financial or health challenges
- Whenever you hear the word "wealth potion" know that it is a sign of a scam

REMEMBER

- There is no shrine or deity with the ability to make you rich.

CAUTION

- Never accompany anyone to a shrine or respond to messages about divinations.

THINK

- Why do these deities need money, can't they offer assistance with out any demands?

Employment Scams

Employment scams are scams which offer jobs that don't exist and is targeted at job seekers with the aim of stealing personal information, obtaining money, deception into joining a sales/multi-level marketing pyramid, or human trafficking/kidnapping. Scammers know that finding a job can be tough, and as such, try to trick job seekers, they advertise where real employers and job placement firms do and make upbeat promises about the chances of employment. However, virtually all of them ask job seekers to pay them for their services before they get a job. Employment scams while having a common theme come in variations, here are a few to keep an eye out for.

E-mailed Job Offer Supposedly from an Employer, Recruiter, or Job Board. This kind of situation occurs when you get a job offer via email for which you did not apply. In some cases, they might even do a brief phone interview for you after which you could get quick feedback and congratulatory email saying you got the job role with a juicy monthly salary, but to continue to the onboarding phase, you must pay for a course/training, software, health insurance cover, etc.

Fake Jobs on social media. Some social networking services (notably Facebook and LinkedIn) have integrated job boards to their platforms so that users can post as well as respond to job offers. Unfortunately, there is nothing stopping a scammer from creating a fake individual or company profile on these platforms and posting fake job offers.

Fake Jobs Impersonating Legitimate Employers. This type of scam occurs when scammers clone the websites of legitimate companies and use fake URLs that are similar to the URLs of the original websites. They then put-up job posts with vague job descriptions and good remunerations to get the attention of job seekers.

Fake Jobs on Legitimate Job Boards. The job board may be a well-known brand name or your favorite professional association's "career center." But, while the job board is legitimate, the job is a SCAM. The fact that a job board requires payment to post jobs does NOT guarantee that all jobs posted on the platform are legitimate. Scammers often make enough money off their scams to cover the cost of the posting, or they may be using a stolen credit card to pay for the posting.

Fake Job Boards. These job boards are owned by scammers. They might display legitimate jobs interspersed with fake jobs to lend credence to the site. Usually, they require your personal information or your personal bank account number so they can begin depositing your paychecks (because they are ready to hire you at once).

Old Acquaintance Job Scam. You receive a text message from someone claiming to be an old school mate or who served in the same state as you during your NYSC days. The person then claims to be privy to a juicy job offer and requests you to send your CV to be sent to the recruiters. Obviously, all this is a sham, and the fake recruiters will ask you for fees to process your application.

Fly-by-night recruitment scam. Fly-by-night recruitment firms set up shop in a location, then advertise vacancies or collect CVs from applicants for a fee with a promise of securing jobs for them, then disappear. They move to a different location and use another name.

Steps for Protection

- Recognize the warning signs that you might be dealing with a Job scam. Such as: you are offered a job without an interview, you're being asked to supply sensitive information before anything else is done, the job is amazingly easy to do and pays very well or no experience is needed.

- Scrutinize Email job offers. The presence of spelling and grammatical errors show that the origin is from an unprofessional entity, most likely scammers. Also, check if the email came from a self-hosted domain. Most legitimate companies have their company domain email e.g., Mike@greatcompany.com while scammers will not want to go through the stress of creating a company domain email and opt for a free email service such as Gmail or Yahoo Mail. Finally, copy and paste a part of the job offer email on a search engine to learn its authenticity. You can include the word "scam" at the end of the search input to detect if anyone has reported that company before as a scam.

- Research, research, research! Always investigate the organization or company by Googling the organization and check what they do exactly and check reviews about the company. Check the CAC website to make sure it's a legit organization or company.

- Never give out your financial information. Never give out details such as your Account Number, BVN, ATM card numbers, or PIN.

- If you're asked for money, run! Don't be in a rush to pay money to get a job no matter how convincing the person may sound, as legitimate companies or organizations won't ask you to pay a certain amount of money to get employed.

REMEMBER

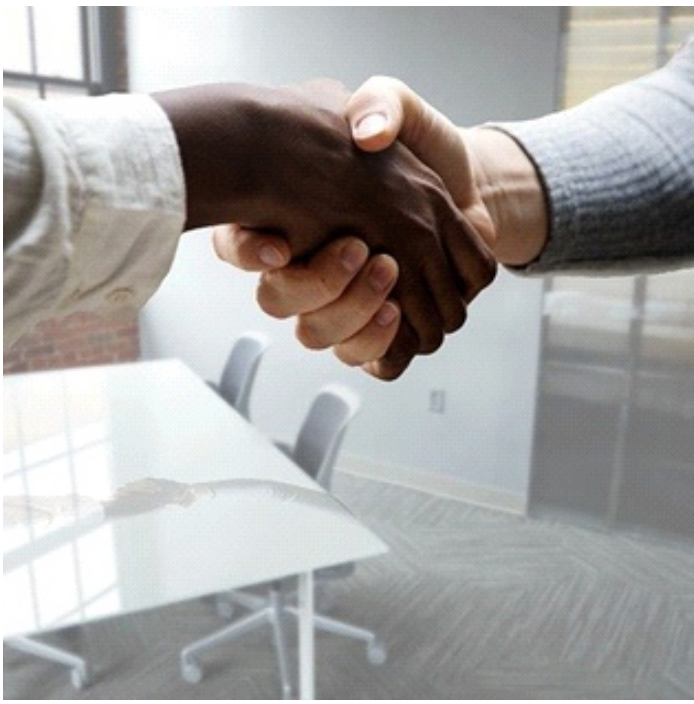
- Legitimate Job Recruiters will never ask you for money.

CAUTION

- Be wary of Job offers with huge salaries, flexible working hours requiring little or no experience.

THINK

- I didn't apply for this job, why am I being invited for an interview?



Immigration Scams

These are scams that prey on the desire to emigrate to other countries in search of better economic and living conditions. These scams can prove costly as you can lose money, get you barred from traveling to the country of your dreams, or get incriminated by the use of your identity to commit fraud. Scammers have various means to commit immigration fraud, but their preferred methods are:

The use of fake websites. Scammers can create a fake website to impersonate a legitimate website of a country's immigration agency. Sometimes they do this by registering a look-alike domain name. For example, the domain to apply online for immigration and citizenship into Canada is https://www.cic.gc.ca and a scammer can register something like https://www.cic.gc.online. These fake websites try to stay as close to the original to fool the unsuspecting.

Fake travel agent. A scammer can pose as a travel agent claiming to have an insider connection with an embassy. They then demand various fees and charges to help obtain travel documents. They either keep up the ruse till the victim is milked dry or they supply fake travel documents.

Visa Lottery scams. These scams play on people's hope of getting in through the Diversity visa lottery program. Scammers can send out an email informing targets that they have won and demand processing fees or sensitive information. Another method is to claim to be able to get targets into the program for a fee.

Steps for Protection

- Do your immigration application yourself instead of contracting it to a third party
- Ignore unsolicited emails, SMS, and social media messages about supposed Immigration officers or agencies
- Confirm from various sources that the domain you have is legitimate and not fake
- If at any time you're in doubt, pay a visit to the embassy or get someone that can go on your behalf to make enquiries

REMEMBER

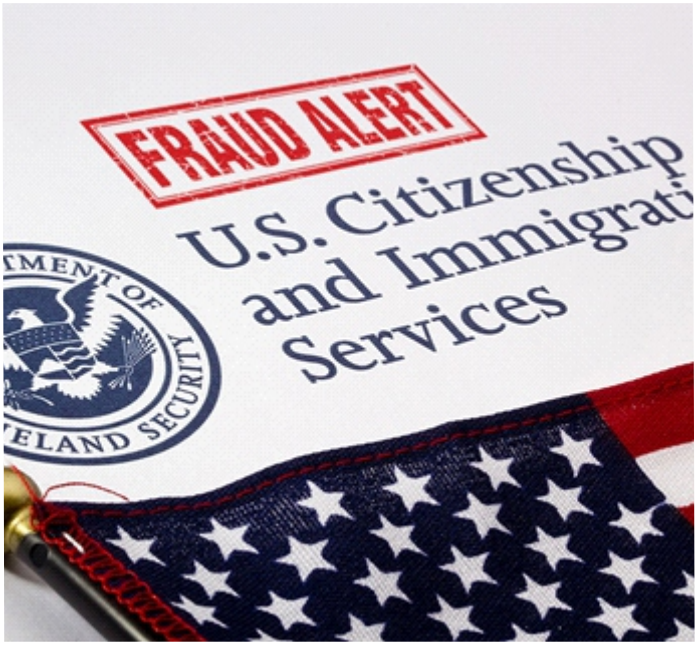
- If you are asked to pay to access application forms and guides, you're dealing with a scam.

CAUTION

- Be wary of guaranteed entry, high paying jobs and deals that are too good to be true.

THINK

- Why pay money to a third party when you can deal directly with the embassy?



Scholarship Scams

These are scams that target those seeking help with higher education. Scholarship scammers set up agencies that claim to "specialize" in getting prospective students full or partial financial aid. Scammers use a variety of means to seek out their targets, from in-person seminars to targeted social media posts and advertisements. Such scammers use a variety of methods to fleece their victims, here are a few:

Scholarship Search Service. In this method, scammers promise to find the best-fit scholarship for a fee and if they don't, you are guaranteed a refund. But as soon as they receive the fee, they disappear. In other cases, they might send you a bogus list of matching scholarships, but their policy is written in such a way that no one can get a refund.

Non Existent Scholarships. Scammers will claim to have found a scholarship for you, but you need to send some money for application or processing. But, the scholarship does not exist, and in the end, they might claim that the scholarship was later canceled, or you didn't qualify.

Financial Aid Lotteries. In essence, this is what these types of scholarships scams are, though the scammers never make this known. How this scam works is that the scammers through their dubious agency will advertise a scholarship of $2000. They take application and processing fees of $50 from say, 1000 applicants. The scammers would make $50,000 and give the scholarship to 3 candidates making a net profit of $44,000. The odds of winning in this scenario are like winning in a lottery.

The Scholarship Prize. You get an email or a message saying you have won a scholarship or have been approved for an educational grant. Of course, the catch here is you need to pay disbursement or redemption fees.

Steps for Protection

- Never pay money to apply or receive a scholarship. If you're being asked to pay for application or processing fees, know that you are dealing with a scammer.
- Never give out financial information like cards and account numbers, if you're being asked for this, you are dealing with a scam.
- If you've been invited to a scholarship seminar, make sure you do a thorough investigation about the agency or organization. Also, never pay money for anything at the venue of the seminar.
- Keep track of the scholarships you've applied for, and if you receive a message that you've been selected for a scholarship you didn't apply for, do not respond.
- Scholarships are not hidden; with a little effort you can find out all the information you need on your own. This is better than letting agents or agencies handle things for you as they might turn out to be a scam.

REMEMBER

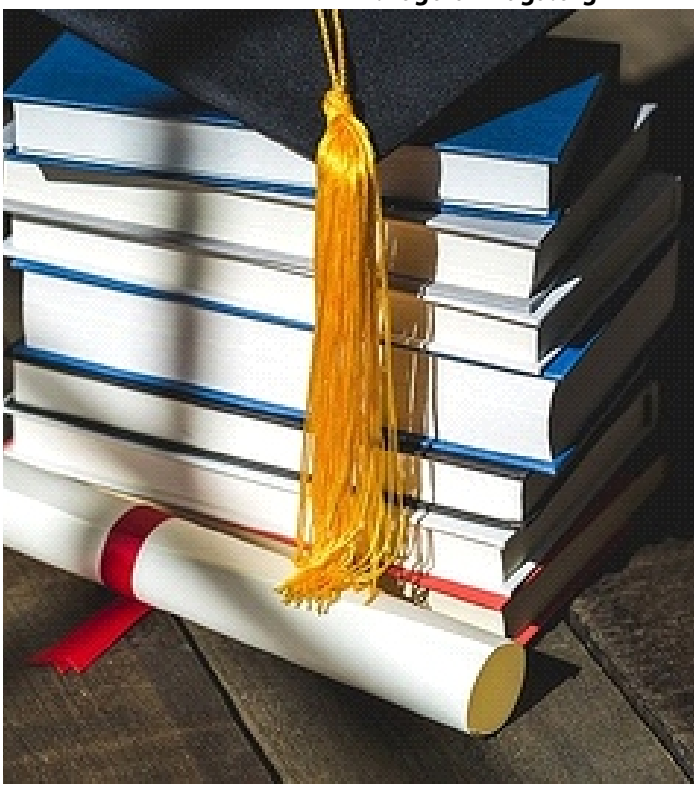
- If you are being asked for money, know that it is a scam.

CAUTION

- Never give out sensitive personal or financial information.

THINK

- Do I really need to pay to get a scholarship, aren't I the one that is suppoed to be paid?



Investment Scams

Investment scams are scams that take advantage of the widespread knowledge that investing can lead to wealth. Scammers then present carefully tailored scams that mimic legitimate investment opportunities with the aim of duping their victims. Investment scams come in all shapes and forms, most common being Ponzi schemes, Pyramid schemes, Pump and Dump Schemes, High Yield Investment Programs, Foreign Currency Trading, Binary Option and Crypto Currency Scams. Prime targets for such schemes are the elderly, the uneducated and people with little or no knowledge about investing. Scammers typically get their victims to comply using various psychological ploys and tricks, below are a few.

Tricks of the trade

- **Creating a fear of missing out.** This is pressure brought on by the urgency of the offer. When the offer is communicated in such a way that implies a time restriction, people are more inclined to act. Another variant of this is when a lot of people have already invested and are being paid "dividends." This would make anyone who was initially skeptical of investing feel like they are missing out.

- **Creating a sense of scarcity.** People are drawn to investment opportunities that tell them that there is nothing like it. Looking around and seeing very few investment opportunities that proclaim the same benefits, people are enticed to throw their hats in.

- **Creating an aura of legitimacy.** Scammers spend a lot of time and effort on appearances. They design sleek and good-looking websites, dress and speak in a professional manner, and may even claim to be affiliated with a reputable organization or financial institution.

- **Feeding the appetite for greed.** Scammers paint vivid pictures and tell stories of those who have made a huge financial windfall from investing with them. They talk about financial security and how the high returns and negligible risk of their investment proposition will lead to a life of financial security. This dangling carrot technique makes sure that the victims keep focusing on the benefits without thinking critically about the obvious risks.

- **Appeal to consensus.** Scammers are quick to claim that a lot of respectable and knowledgeable people have already bought into their scheme, they can even present a religious leader or celebrity as the face of the scheme.

Steps for Protection

- **Don't invest if there is talk of guaranteed returns.** There is no such thing as a guaranteed return on investment. All investments have risk. Hence, any investment offer that claims there is no risk or minimal risk while promising high returns is a scam. Keep this in mind, high returns are associated with considerable risk and low returns are associated with minimal risk.

- **Don't invest in what you can't understand.** When asked how the scheme works or how they generate the income to pay dividends, investment scammers might use jargon or give an explanation

that is incomprehensible due to its complexity. Don't put money into something you don't understand.

- **Do your due diligence.** Conduct a thorough research of the investment offer. Do a background check on the individuals and organizations behind it. Finally, seek expert advice before making any financial commitment.

- **Don't invest if they are not licensed.** Most fraudulent schemes are unregistered and unlicensed. A legitimate investment firm should be registered with the relevant authorities in the country where they operate. For instance, if the firm is operating in Nigeria, it should be registered with the Securities and Exchange Commission.

- **Compare prevalent market rates.** Compare promised dividends with current industry rate. Is it higher than what other investment firms are paying out? Is it higher than Fixed deposit rate? Is it higher than the CBN's Monetary Policy Rate?

REMEMBER

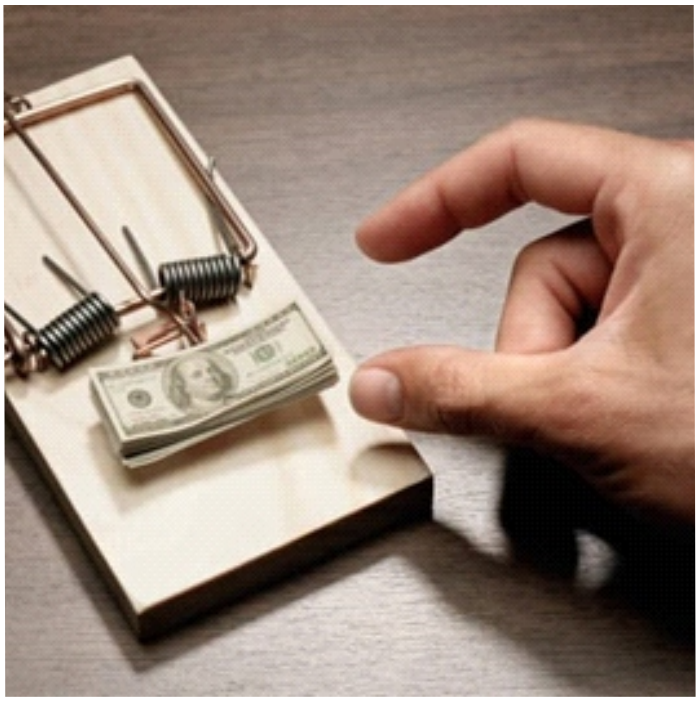
- Investments offers that guarantee returns with no risk do not exist.

CAUTION

- Do not be quick to commit financially to an investment offer. Only do so after extensive investigation and consultation.

THINK

- If you're being pressured, ask yourself. "Am I okay with losing all of my money?"



Extractive Industries Scams

These are scams that use the extractive industries, the business of taking raw materials, including oil, coal, gold, iron, copper, and other minerals from the earth as a pretext to fleece unsuspecting victims. Scammers that play in this sector are usually sophisticated and have taken the time to study the inner workings of the industry. They might put up websites or contact potential victims via email or phone calls claiming others have made a huge financial windfall by investing in the extractive industries. They often supply samples and fake documentation to convince potential victims.

Common examples of extractive industries scams are crude oil and mining scams. In these scams, either the scammers are offering the products below their market price to the potential victims, or the scammers are asking them to invest in mining the products at incredibly low costs to sell at the prevailing market rate and make huge profits.

Steps for Protection

- Ignore unsolicited phone calls and emails. If you receive an unsolicited phone call or email about a Crude Oil/mineral resources investment, do not respond.
- Do your due diligence. Thoroughly investigate both the individual and the offer.
- Don't be swayed by the talk of limited opportunities and deadlines. The usual mode of operation of Scammers is that they try to give you the impression that the "opportunity" they are promoting is limited and scarce.

REMEMBER

- Do your research. Verify information with the relevant govenment and state agencies that regulate the extractive industries.

CAUTION

- Illegal minning and refining are a major issue with the extractive industries. The scammer can use this to try and silience you by claiming your funds were invested in an illegal operation, so reporting would be putting yourself at odds with the law.

THINK

- Is this person authorized to sell this mineral resource?

Email Scams

E-mail is still one of the most popular means of communication for both businesses and individuals. As such, scammers have adapted various scams to fit it to reach a large number of people. Below are three popular email scams you're sure to come across.

Advanced fee fraud. Unfortunately, these have been dubbed "Nigerian Prince" email scams, even though the origin dates to the 19th-century Spanish prisoner scam. The premise hasn't changed, a scammer poses as a person of wealth whose money is trapped somewhere and needs help to get it out, and is willing to offer a handsome reward. They will request your bank account details to transfer the money and a small fee they need to pay to bribe officials to get the money released. Of course, there are many variations to this as scammers have various stories all around the same theme.

Bank Impersonation. The aim of this scam is to get sensitive bank information. Scammers send emails with bank logos and branding; this email might claim some sort of maintenance is occurring on your account and the bank needs to verify your information. They might also use scare tactics, such as claiming a huge debit has occurred on your account, all in a bid to get you to click a link. The link takes you to a page that has been designed to look exactly like your bank's website, there you are then asked to enter your financial details.

Service Impersonation. These scams specifically target card details. Scammers know a lot of people subscribe to assorted services using their card, so they would send an email impersonating the vendor (e.g., Netflix) saying there has been an issue and you need to re-enter your card details. Like the earlier scam, the email comes with that leads to a webpage that has been designed to look like that of the vendor.

Steps For Protection

- **The Use of fear and urgency.** Pause and look at the e-mail again. Is it using scare tactics to get you to take an action? Are you being asked to do something in a short time frame else a bad consequence will occur? If any of these are present know you are dealing with an email scam.
- **Check the sender's address.** You can do this by hovering your mouse over the "from" address. If you see more numbers or letter added to the company domain (e.g., support@multichoice 123.com instead of support@multichoice.com), you're dealing with an email scam.
- **Check for grammatical and spelling errors.** The presence of such shows you might be dealing with a scam.
- **Is it a service you use?** A service or vendor you don't use won't just send you an email without you first contacting them. So, if you receive such, it most likely a scam.
- **Don't click links you didn't ask for.** For example, if you're expecting an email from a

co-worker with a link to a service then that's okay. Any email with a link you're not expecting should be treated with caution. If you need to check the link, right-click and copy and paste it on VirusTotal: http;//www.virustotal.com/gui/home/url

- **Don't open Email attachments you didn't ask for.** If you received an email with an attachment, you didn't explicitly ask for, contact the sender (via phone or some other means) to confirm if they're the ones that sent it.

- **Use anti-phishing tools.** Consider only opening emails from a web browser with an anti-phishing extension.

REMEMBER

- No legitimate organization will ask you for your password, pin or card details via email.

CAUTION

- Treat any email that contains a link or attachment with extreme caution.

THINK

- If an email is requesting for you to take an action, pause. Ask youself, is what I am being asked to do really make sense?

Mobile Phone Scams

Mobile phone scams are scams using a mobile phone, often through phone calls or text messages. Scams perpetrated through calls are known as Vishing while those through text messaging are called Smishing. Both are forms of Phishing, which is the use of deception to obtain sensitive information. The goal of the scammers is a monetary payoff. This is done by selling the information to a third party with malicious intent or using it to defraud the victim. Below are some common tricks used by mobile phone scammers.

Asking victims to "confirm" financial information. For instance, you might receive a call from a scammer posing as a customer support agent of your bank. The scammer then claims that due to maintenance being done on your account, he would need to confirm your account details. The scammer proceeds to call out details such as your name and date of birth obtained from a leak. After you confirm the information as true, the scammer will ask that you call out your ATM card number to confirm if it matches what they have on their records. The goal here is to trick you into revealing sensitive financial information using information about you from other sources.

Impersonating acquaintances from the past. Scammers might call you or send you a text claiming to be a classmate from school or an acquaintance from NYSC. They would then present a bogus scheme to extract money or sensitive information.

Use of fear and urgency. Scammers might send you a text message right before the start of a holiday that your account will be blocked if you do not take their prescribed action. They aim to get you to panic and take an action due to the knowledge that once the holiday starts no one at the bank will be able to attend to you.

Pretending to help solve a problem that doesn't exist. Scammers can call pretending to be from your bank and claim that there's been some unusual activity on your account that resembles a fraudulent transaction. They will then proceed to ask you to disclose your financial details, so the attempt can be stopped.

Steps for Protection

- Never, under any circumstance, disclose your financial data (e.g., OTP, account number, online banking username and/or password, ATM PIN, Debit card number, CVV, BVN, etc.) to anyone over the phone or via text message.
- Always keep in mind that no financial institution or organization will request sensitive information via a phone call or text message.
- If you have received a text message or a call from someone claiming to be from your financial institution, do not act at once. In the case of a call, hang up, then call the customer service number provided by your bank to confirm if the communication was from them.

- If you receive a text message asking you to click a link do not do so except you are expecting or asked for it.
- Slow down if a message is urgent. You should approach urgent account updates and limited time offers as caution signs of possible smishing. Remain skeptical and continue carefully.
- Check the phone number. Odd-looking phone numbers, such as 4-digit ones, can be evidence of email-to-text services. This is one of many tactics a scammer can use to mask their true phone number.

REMEMBER

- Your Bank will never ask for your financial details via phone calls or text messages.

CAUTION

- Never provide a password or account recovery code via text to anyone.

THINK

- Is this call or message trying to make me take an immediate action?

Social Media Scams

Social media scams are scams that use a particular social media platform to defraud the users of that platform. Due to the almost universal use of social media, scammers have found it a helpful tool for scouting potential victims and for the propagation of their scams. Several of the scams covered in this volume have a slight variation adapted for propagation on social media. Also, scammers often use social media as the originating point for their schemes, this is done by paying for catchy ads and embedding them with links to the fraudulent schemes. Below are some common scams you're likely to come across on social media.

Money flipping scams from hijacked accounts. The scam starts with a scammer hijacking someone's account. Once the account is under the full control of the scammer, the scammers does a post about an investment scheme that yields double of what was invested and tags all the friends of the hijacked account.

Romance Scammers. Aside from dating sites, social media is another tool for romance scammers. They create legitimate looking profiles to defraud those looking for love or relationships.

Influencer scam. Influencers are those on social media with a large following. Unfortunately, some of these individuals resort to less than worthy practices to monetize their followership. Influences have been caught promoting Ponzi scams or disappearing with funds after asking their followers to invest in a business scheme.

Fake celebrity scam. A scammer impersonates a celebrity and does a post announcing a giveaway. The supposed "winners" are then contacted to redeem their prizes by paying a delivery fee for the item and supplying other information. Once the delivery fee is paid, the scammer blocks the victims and sometimes sells their information to other scammers. Another variant of this is when the scammers use the fake celebrity profile to promote a Ponzi or investment scam.

Fake Vendor scam. Scammers pose as vendors or service providers, once a victim pays money for a good or service they are blocked. Another variant of this is when a scammer impersonates a vendor or business on social media. Since the scammers are using the same logos and pictures as the legitimate vendors, those who do a search on social media and land on the fake accounts are defrauded.

Auction scams. Scammers impersonate government agencies and put-up posts about goods to be auctioned. A favorite for scammers is impersonating officers of the Nigeria Customs service. Often, you'll come across profiles of supposed Customs officials with posts about cars to be auctioned at prices way below their market value.

Steps For Protection

- Regularly check and update the privacy settings of your social media account. Limit who can see your posts, pictures and the information displayed on your profile.

- Be careful what you post about yourself and your activities, do not share personal information on social media.

- Do not accept friend requests from people you don't know.
- Use a strong password and set up two factor authentication.
- Don't partake in social media challenges and quizzes, especially those that ask questions that are personal.
- Always do a search using the profile or page name of the company on social media. If you see multiple accounts do not continue till you can figure out which, if any, are genuine. Note that cybercriminals also seek out businesses that do not have a social media presence to impersonate, hence seeing only one account does not mean that it is genuine.
- Be wary of Investment offers being promoted on social media. Do not invest till you have sought advice from competent and certified investment professionals.

REMEMBER

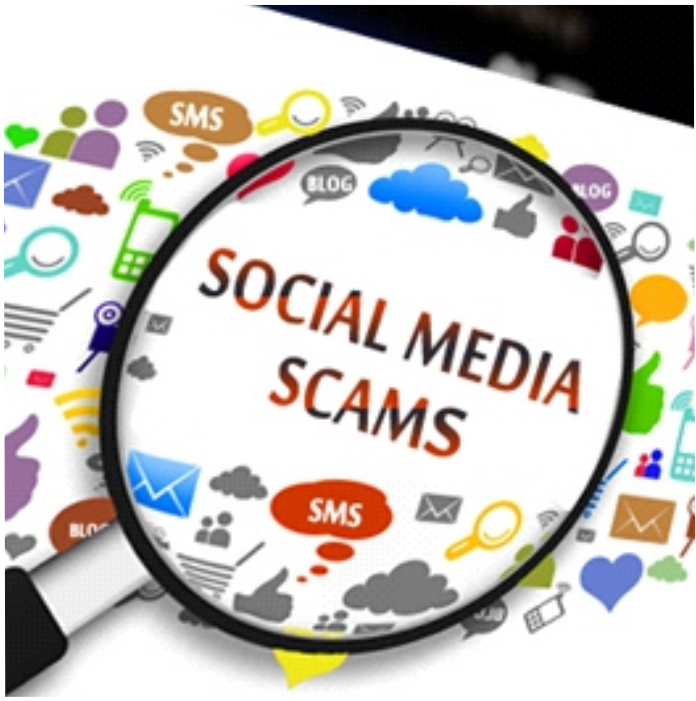
- Do a thorough research of any account you plan on having financial dealings with on social media.

CAUTION

- Be careful abot what you post on your social media handles.

THINK

- Can I trust someone with my money whom I only know through social media?



What To Do **If You Get Scammed**

Once you discover that you have been scammed or you suspect that you have been scammed, then time is of the essence. This is because there is still a possibility that you can recover your money or limit the damage that has been done. Here are some steps you can take.

- **If you suspect someone has access to your card details.** Always keep the customer service numbers for your financial institution handy. Once you notice unauthorized withdrawals, call the numbers to block the card at once and suspend any further activity on your account.

- **If you suspect someone has access to your PC or Mobile Phone.** If you suspect someone has or had access to your online banking portal or mobile app via your PC or Mobile Phone, call your financial institution to report your suspicions. Install a paid anti-malware solution and run a full system scan. Then change the passwords associated with your online and mobile banking profiles.

- **If you suspect the person you sent money to may be a scammer.** Immediately call your financial institution to see if there is any possibility that the transaction might be cancelled if it is still pending. If the transaction has been consummated, then get the necessary documents, such as a police report and court affidavit to lodge a complaint with your financial institution.

Report the Incident

If you have been scammed, it is important to report the incident. This is because if you do not report the incident, the relevant authorities will not be able to do anything about it, and you expose countless others who are in a similar position to yourself to be preyed upon by the same fraudsters. By reporting the incident, the authorities can act, either by sensitizing the public or going after the scammers, ensuring that others will not suffer a similar fate as you. Below are some reporting channels you or anyone you know who has been scammed can make use of.

Nigeria Police Force Cybercrime Reporting Portal
- **Website:** https://incb.npf.gov.ng/
- **Phone Number:** +234 80 9455 9845
- **Email:** interpolnigeria@npf.gov.ng

Economic and Financial Crimes Commission
- **Website:** https://www.efccnigeria.org/
- **Mobile App:** Eagle Eye (EFCC)

No Go Fall Maga
- **Website:** https://nogofallmaga.org/report-scam/

Final Word

In conclusion, please bear in mind that this booklet does not have all the answers. Learn to be skeptical and ask a lot of questions, especially when money, a prized asset or sensitive information is involved. Be suspicious and remember if it sounds too good to be true it probably is!

Contributors

- Praise Sunday
- Ayodele Jonathan
- Gideon Tiamiyu
- Shuaib Oseni
- Oluwabunmi Adeyemo
- Oghenetega Okukulabe

Editor
Enyinna Abazie

NoGo FallMaga

www.nogofallmaga.org

cybersafe. FOUNDATION | tell two