Financial
PROTECTION

More about

Scams

Introduction

Before we even consider discussing investment plans, let's start by warning you about the possibility that someone may try to trick you into investing money with them, with the express intention of stealing your money. This is called a scam.

Legitimate companies with trustworthy façades are used by con-men to instil confidence in their victims.

Rented office spaces, receptionists, professionally designed brochures, impressive websites, and more, are all tools used to create the appearance of legitimacy.

That's because the con artist knows he or she must gain your trust to get your money, so he or she will do everything necessary to appear reputable.

1. Personal data

To avoid being caught out by a scam, make sure you follow these simple rules.
Reject any unsolicited calls, emails, text messages or visitors to your door.

- Check with the FSCA if the company is registered.
- If you are thinking about an investment opportunity, seek independent financial advice from an authorised FSCA financial advisor.
- Always take care of personal data.

Note: Phishing is a form of fraud in which an attacker pretends to be a reputable entity or person in email or other communication channels.

In computing, SMS phishing or "smishing" is a form of criminal activity using social engineering techniques. Phishing is the act of attempting to acquire personal information such as passwords and details by masquerading as a trustworthy entity in an electronic communication.

Note: Never answer an SMS if you are not 100% sure of the originator.

2. Types of investment scams

Investment fraud can take many shapes and forms, but when we look to categorise them, they fall into the following categories:

- Pyramid schemes
- Ponzi schemes
- Pump-and-dump
- Advance fee fraud
- Offshore scams
- SMS phishing
- Identity fraud
- Online gift
- Travel fraud
- Job Scam
- Truck scam
- Property Scam
- Investment scams

2.1 Pyramid schemes

In this scheme, fraudsters claim to turn small investments into large profits within a short period of time. However, the truth behind this investment is that "investors" are paid dividends from money contributed by new participants to the programme. Each "investor" to the programme, has to recruit a specified number of new participants to allow them to "move up" the ladder.

Pyramid schemes usually fall apart when it becomes impossible to recruit new participants.

Investment	Pyramid Scheme
A consumer is not required to recruit other participants to the scheme.	Participants are always required to recruit others into the scheme and are promised huge returns within a short period of time.
A consumer knows where his / her monies are invested and the rate of return.	Money simply exchanges hands with no real economic activity or products attached to it. Where products are sold, they are simply a smoke screen to hide the pyramid scheme. Significant returns are derived from the recruitment of participants and not from the actual sale of the product.
Investment broker is registered with the FSCA.	Promoters are not registered anywhere.
Broker is traceable and accountable for his / her actions and advice.	No means of tracing the scheme or promoter's origins.
Legal and safe way of investing money.	It is illegal to participate or promote a pyramid scheme. Participants risk losing money.
Recourse mechanisms available.	Hardly any recourse.

2.2 Ponzi schemes

In this scheme, a central fraudster collects money from new investors and uses it to pay dividends to early-stage investors, rather than investing it or managing it as intended.

The only difference between a Pyramid Scheme and a Ponzi Scheme is that within the Ponzi Scheme the investors do not have to recruit additional participants. Ponzi Schemes collapse when too many investors want to withdraw their money at the same time, or when it becomes too difficult to attract new investors.

2.3 Pump-and-dump fraud

In this scheme, a fraudster will deliberately buy shares of a very low-priced stock of a small, thinly traded company. The fraudster then proceeds to spread false information about the company, which in turn increases the interest in the stock, which increases the stock price.

Investors then creates a buying demand, as they believe that they are getting a good value for money. This pushes the price of the stock up even more.

Then the fraudster dumps his or her shares at the high price and disappears, leaving many people caught with worthless shares of stock.

2.4 Advance fee fraud

This fraud plays on an investor's hope that he or she can rectify a previous investment mistake by purchasing low-priced stock. The scam begins with an offer to pay a high price for worthless stock in your portfolio. However, you will have to pay a fee in advance for this service. Needless to say, if you do pay this fee, you will never see that money again.

2.5 Offshore scams

These scams can take a number of forms and are often a combination of these mentioned above. These scams promise huge profits and tax concessions if funds are invested in another country.

2.6 SMS phishing

In computing, SMS phishing or smishing is a form of criminal activity using social engineering techniques. Phishing is the act of trying to get your personal information such as passwords and details by posing to be a trustworthy entity in an electronic communication.

Note: Never answer an SMS if you are not 100% sure of the originator.

2.7 Identity fraud

Identity fraud is the use by one person of another person's personal information, without them knowing, to commit a crime or to deceive or defraud that person.

Note: Never give out your personal information to any unauthorised person

2.8 Online gift

While many online sellers are legitimate, unfortunately, scammers can use the anonymous nature of the internet to rip off unsuspecting shoppers.

Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores. They may use sophisticated designs and layouts, possibly stolen logos.

Many of these websites offer luxury items such as popular brands of clothing, jewellery and electronics at very low prices. Sometimes you will receive the item you paid for, but they will be fake, other times you will receive nothing at all.

The biggest tip-off that a retail website is a scam is the method of payment. Scammers will often ask you to pay using a money order, pre-loaded money card, or wire transfer, but if you send your money this way, it is unlikely you will see it again or receive your purchased item.

A newer version of online shopping scams involves the use of social media platforms to set up fake online stores. They open the store for a short time, often selling fake branded clothing or jewellery.
After making a number of sales, the stores disappear. They also use social media to advertise their fake website, so do not trust a site just because you have seen it advertised or shared on social media. The best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing.

Warning signs

- A product is advertised at an unbelievably low price, or advertised to have amazing benefits or features that sound too good to be true.
- The other party insists on immediate payment or payment by electronic funds transfer or a wire service. They may insist that you pay up-front for vouchers before you can access a cheap deal or a giveaway.
- The social media-based store is very new and selling products at very low prices. The store may have limited information about delivery and other policies.

- An online retailer does not provide adequate information about privacy, terms and conditions of use, dispute resolution or contact details. The seller may be based overseas, or the seller does not allow payment through a secure payment service such as PayPal or a credit card transaction.

2.9 Travel fraud

The thought of going to a warm vacation spot in the winter or visiting a foreign country is exciting. But what seems like a great deal may turn out to be a bad trip.

- Be sceptical of offers for "free" trips. Airlines and other well-known companies sometimes operate contests for travel prizes. However, there are also companies that offer "free" trips to try to lure people into buying their products or services. It is never "free" if you have to pay something.
- Know exactly what's included. A "free" or incredibly cheap trip may have hidden costs. For instance, the cruise may be free, but you have to pay to fly to the departure point and stay in a hotel at your own expense. Or you may have to endure a long, high-pressure sales pitch for a timeshare or travel club membership as part of the trip.
- Realise that the deal may not be as good as you think. You may find that a travel offer requires you to make reservations through a specific company and that the costs are higher than they would be if you used your own travel agent or made the arrangements yourself. Or the offer may be valid only if you bring a companion along at full fare.
- Be aware of restrictions. Often the best travel deals are only available for off-peak times, not during school vacations, holidays or other popular travel dates. You may find it hard to get the promised price for the dates that you want to travel, or there may be no space available on those dates at all.
- Confirm the arrangements. If transportation and hotel are included in the travel package, ask how to contact those companies and confirm with them directly that the reservations have been made.
- Do your own travel research. It is easy to get information from a local travel agent and other sources such as trusted Websites and the Internet. You may be able to get the trip you want for far less than the "bargain" price a company is offering.
- Payment. Fraudulent travel operators take the money and run, and even legitimate companies can suddenly go out of business. Some places allow you to reserve without your credit card. If working through a travel agent, this can also be done. Look for options of paying cash on arrival.

Note: You can go online and look at credible travel websites for reviews from other travelers. You can also Google maps the area and see if they are legit.

2.10 Job Scam

When you are unemployed and desperate for a job, it is important that you are aware that people could try and scam you into thinking you are getting a job. The conversation would normally require you to pay a fee to get the job.

Here are some tips to help you identify fake job offers and avoid job scams. Internet fraud is rampant, and scammers prey on job seekers. Your best defence is to do your research and report internet job scams.

Below are the things to look at:

- Too good to be true – They contacted you, and the pay is way higher than you expected, you can also start immediately.
- Vague job requirements and job description – The job description is written in such a way that almost anyone could apply for the job. A real job requirement will be quite specific.

- Unprofessional emails – There will be mistakes with the spelling, punctuation and grammar in the email. There could also be an overuse of capitals and colours.
- Online interviews – Interviews using Yahoo instant messenger or other instant messaging service.
- Emails do not include contact details.
- You are asked to pay a fee for the job.
- You are required to give out all your personal information like bank details.
- Job asks for an upfront payment to guarantee you the job.

2.11 Truck scam

An advert is placed for a truck and trailer. Interested buyers will try and get a hold of the advertiser – in many cases because the item is advertised for such a low price. Trying the number listed and, eventually opting for the 'Email Dealer' option, the interested buyer will finally get a reply from the advertiser via email.

When asked why he or she is not available via telephone, the advertiser comes up with a plausible excuse, saying that he or she is out of the country at the moment and cannot use their cell phone.

After communicating via email, the advertiser will ask the interested party to pay a deposit for the advertised item into an account. After paying the deposit, the advertiser either disappears or asks for more money before the item can be released to the buyer.

Note the following:
- Never pay a deposit before you have viewed the truck and trailer
- Examine the invoice for small details like spelling mistakes, website addresses, physical addresses, Vat number
- If in doubt walk away and do not part with your money.

2.12 Property Scam

Property scams include:
- Renting of properties that do not exist
- Selling properties that are not for sale
- A person wanting to buy your property even though it is not on the market

When renting or purchasing a property keep note of the following:
- Be wary of payment requests
- Too-good prices
- The email sounds strange
- The agent won't show you the property
- The seller pushes you
- The seller asks you to wire money
- The buyer or seller is foreign and wants to buy a home unseen
- Know market-related prices
- Always question a 'bargain.'
- Don't be rushed
- Always view the property before paying

3. Internet

The changing face of communications technology provides new tools for the investment scam artist to exploit. First was mail, and then the telegraph became a popular tool for investment scammers. Next was the telephone, and now it is the Internet.

The Internet has made investment fraud more efficient and effective. Con artists can purchase lists of targeted groups, use automated data-gathering tools, and post to discussion groups at almost no cost and with complete anonymity.

With a few clicks of a mouse, fraudsters can reach millions of people by building a website or entering various chat rooms. One person could use many of these web-related tools under various aliases to cheaply and easily create a virtual facade of legitimacy with little risk of detection.

Another example of Internet investment fraud is online newsletter publishers who are paid cash and securities to tout certain stocks (attempt to sell (something), typically by a direct or persistent approach).

This is not illegal; however, the biased advice must be disclosed. Watch out for newsletters that bury information about who paid them, the amount, and the type of payment in fine print, so you never see it.

You should verify all investment advice from unknown sources online by checking reputable sources offline – be sceptical. Remember, almost anyone can make himself appear to be an established and successful company for very little cost, online.

Note: Be cautious as to what you post on social media. Some scammers will call you and mention things from your social media to trick you into believing them.

3.1 Emails

In emails look out for the following:

- Look at the email address to see if there is anything strange for example the sender is from North Bank, but if you look at the email address, it has a Gmail account from a completely different name.
- Check links in the email. Hover your mouse over them, do not click them. Delete the email.
- Check for spelling mistakes.
- Analyse the salutation. For example “valued customer”, a legitimate business would use your name.
- Beware of urgent or threatening language.
- Review the signature. Lack of details about the signer or how to contact them suggests phishing (a fraudulent practice of sending emails pretending to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers).

Remember:

- Never give out any personal information
- Never click on a link
- Never respond
- Do not believe everything you see

4. Red flags

4.1 Signs of a scam

There are a number of giveaway clues that the investment could be a scam

- It is too good to be true
- Guarantees - be suspicious of anyone who guarantees you a return. Investment will always carry a degree of risk
- Unregistered advisors - many scams involve unlicensed advisors selling unregistered investments, including shares, bonds, hedge funds and other fictitious instruments
- Overly consistent returns - be cautious of investments that go up month after month, or that provide remarkably steady returns irrespective of the market conditions
- Complex strategies - avoid anyone who credits their success with a highly complex investing technique. If they can't explain it clearly, walk away
- Missing documentation - if someone tries to sell you an investment without a prospectus or an offering circular he or she may be selling an unregistered investment
- Pushy salesman - if someone pressures you to decide on a stock sale or purchase, walk away. This may not necessarily be an indication of fraud, but it's poor business practice

Note: It is always wise to seek financial advice from an authorised financial adviser when investing.

4.2 Features of scams

Some scammers have very convincing websites and other online presence, which makes them look like a legitimate company. Always check with the FSCA to make sure they are registered.

Make sure you are aware of the warning signs, which might indicate an investment opportunity is a scam.
Unsolicited approaches by phone call, text message, email or a person knocking on your door.
When a firm does not allow you to call it back.
Where you are forced to make a quick decision or are pressured into doing so.
Contact details you are given, or on their website are only mobile phone numbers or a PO box address.
You are being offered a high return on your investment, but are told it is low risk.
They are very confident, convincing and well dressed.

NOTE: Scammers are always figuring out new ways in which to scam consumers out of their hard earned money. You need to be vigilant and do not be afraid to ask questions.

5. Report scams and fraud

Ombud Offices in South Africa / Places in SA to take your complaint to:
With effect from 1 April 2005, any scheme established by a financial institution or group of financial institutions to resolve a client's complaint by an Ombud has to be recognised by the Financial Services Ombud Schemes Council. This Council was established in terms of the Financial Services Ombud Schemes Act, 37 of 2004. The functions of the Council include the promotion of co-operation of Ombud Schemes, the promotion of best practices for complaint resolution and ensuring the independence and impartiality of Ombudsmen.

You can check if you have been targeted by calling

Tel: 0800 333 437
email: report@easycomeeasygo.co.za
web: www.easycomeeasygo.co.za

Financial Sector Conduct Authority (FSCA)

To check if an FSP or financial advisor is authorised to sell you financial products and services, you can contact the FSCA:

Tel: 012 428 8000
Fax: 012 346 6941
Call centre: 0800 20 FSCA (3722)

E-mail: info@fsca.co.za
Website: www.fsca.co.za

South African Police Services (SAPS)

If you have any information on a scam, you can contact the South African Police Services:

Commercial Crime Unit:
(Enquiries regarding transaction purportedly originating from the South African government agencies or financial institutions)

Tel: 012 339 1203
Fax: 012 339 1202

Crime stop: 0860 010 111 (TIP-OFF)

South African Reserve Bank (SARB)

If you have any information on a scam, you can contact the South African Reserve Bank:

Tel: 012 399 796

Website: www.resbank.co.za

The National Consumer Commission

If you have any information on a scam, you can contact the South African Reserve Bank:

Call Centre: 012 428 7000
Website: www.thencc.gov.za

Email: Complaints@thencc.org.za

Ombudsman for Long-term Insurance

If you have a complaint against an insurer about life insurance, funeral cover and other long-term insurance matters and you are unhappy with their response to your complaint. You can make contact with the Ombud:

Email: info@ombud.co.za
Tel: 021 657 5000
Sharecall: 0860 103 236
Fax: 021 674 0951
Website: www.ombud.co.za

Ombudsman for Short-term Insurance (OSTI)

If you have a complaint against a short-term insurance company and you are unhappy with their response to your complaint. You can contact the Ombudsman for Short-term insurance:

Email: info@osti.co.za
Tel: 011 726 8900
Sharecall: 0860 726 890
Fax: 011 726 5501
Website: www.osti.co.za

Ombudsman for Banking Services (OBS)

The OBS resolves individual complaints about banking service and products. If you have followed the banks complaints process and your complaints fall within the BBS jurisdiction, you can contact the OBS:

Email: info@obssa.co.za
Complaints:
https://www.obssa.co.za/resolving-complaints/how-to-complain/
Tel: 011 712 1800
Sharecall: 0860 800 900
Fax: 012 348 3447 / 012 470 9097 / 086 764 1422
Website: www.obssa.co.za

Credit Ombud (previously known as the Credit Information Ombud)

The office of the Credit Ombudsman resolves complaints from consumers and businesses that are negatively impacted by credit bureau information or when a consumer has a dispute with a credit provider.

Email: ombud@creditombud.org.za
Call centre: 0861 662 837
Tel: 011 781 6431
Fax: 086 674 7414
Website: www.creditombud.org.za

SMS "HELP" to 44786

The Pension Funds Adjudicator (PFA)

If you have a complaint against your pension, provident, preservation or retirement fund that you have not been able to resolve with your employer, you may lodge a complaint with the PFA in writing.

41 Matroosberg Road, Ashlea Gardens
Ext 6, 0081
Call centre: 086 066 2837
Tel: 012 346 1738 / 012 748 4000

Fax: 086 693 7472
E-mail: enquiries@pfa.org.za
Website: www.pfa.org.za

Ombudsman for Financial Services Providers (FAIS Ombud)

Do you have a complaint against a product provider or financial advisor?

Enquiries on status of complaints: enquiries@faisombud.co.za
Sharecall: 086 066 3247
Tel: 012 762 5000 / 012 470 9080

Fax: 012 348 3447
E-mail: info@faisombud.co.za
P.O Box 74571, Lynnwood Ridge, 0040
Website: www.faisombud.co.za

Government Employee Pension Fund (GEPF)

The GEPF manages and administers pensions and other benefits for government employees in South Africa. If you have any complaints regarding your pension and you work for South African government, contact the GEPF:

Toll-free if you are calling from a landline:
0800 117 669
Fraud Helpline: 0800 203 900
Fax: 012 326 2507

E-mail: enquiries@gepf.co.za /
gautengenquiries@@gpaa.gov.za
Website: www.gepf.gov.za

Johannesburg Securities Exchange Complaints and Dispute Scheme

This Office can be contacted at:

The Surveillance Department of the JSE Ltd
Private Bag X991174, Sandton, 2146
One Exchange Square, Gwen Lane, Sandown, 2196
Tel: 011 520 7000

Fax: 011 520 8605
E-mail: Surveillance@jse.co.za
Website: www.jse.co.za