Financial PROTECTION

SCAMS

FSCA MyMoney Learning Series

FSCA
Financial Sector Conduct Authority

Content

Don't fall victim to a scam!

To avoid being caught out by a scam, follow these simple rules:

- If an investment opportunity sounds too good to be true, it generally is. Seek independent financial advice from an authorised financial advisor.
- If you have to make a payment upfront to claim a prize or get access to lottery money this is usually a sign that this is a scam.
- If a telemarketer calls you and asks you for your personal information such as your ID number, Pin or banking details, this is also a sign of a scam. No Bank will ask you for this information over the telephone.
- If you are in doubt, rather wait until you have more information so that you can respond in an informed and educated manner before parting with your hard earned money.

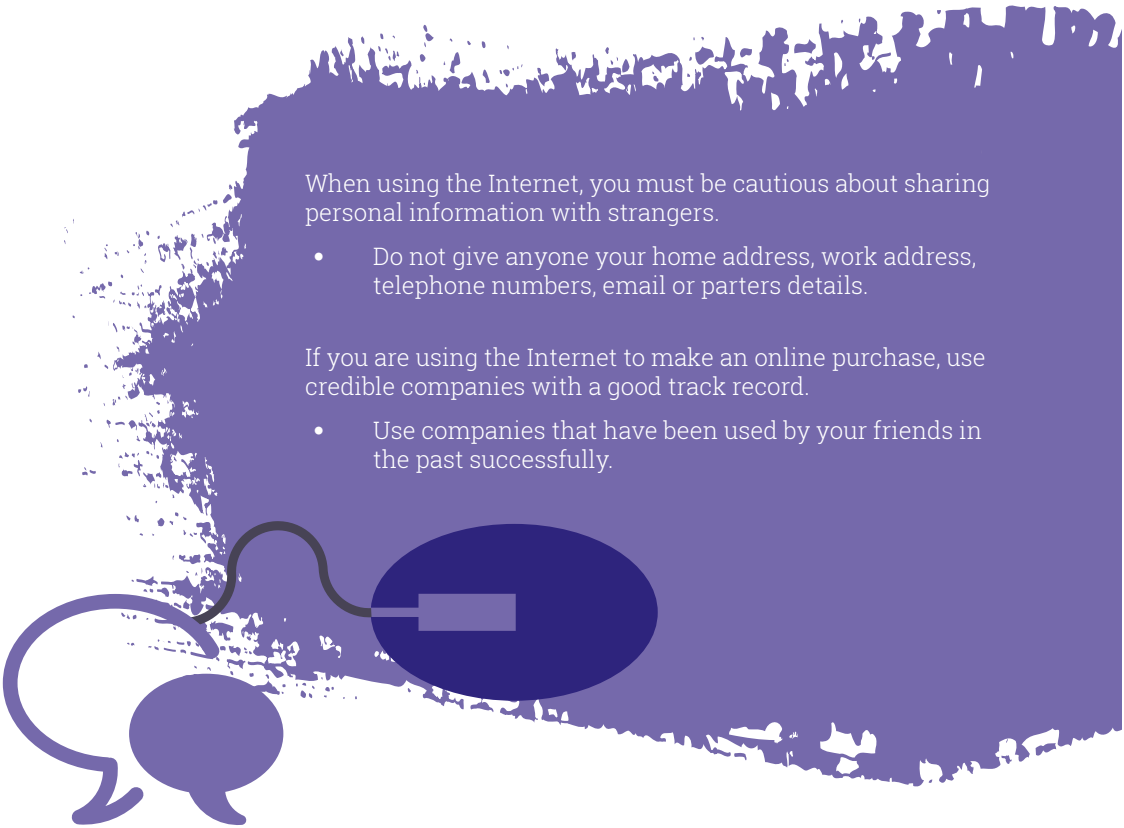
Keep your personal financial information like your bank account number, pin and verification passwords PRIVATE and to yourself.

Do not respond to emails or SMS's that request your personal information such as your bank account number or pin code.

The internet

The Internet has made it easier to defraud people all over the world. Remember a con artist, isn't a man in a black mask. These con artists look just like you and me, except for the fact that they want to steal your hard earned money. 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 different names to cheaply and easily create a fake website that looks real with little risk of detection.



When using the Internet, you must be cautious about sharing personal information with strangers.

- Do not give anyone your home address, work address, telephone numbers, email or parters details.

If you are using the Internet to make an online purchase, use credible companies with a good track record.

- Use companies that have been used by your friends in the past successfully.

Don't fall victim to a scam!

Remember:

- Never give out any personal information.
- Avoid clicking on a link in an SMS or e-mail as this can allow scam artists to get your personal information from your phone or computer devices without you even providing it.
- If you sense a red flag, end the call and block the number.
- Do not believe everything you see.

Emails

Fraudsters often use emails to scam people. Always be aware and look out for things like…

- The email address – is there 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 the links in the email. Hover your mouse over them, do not click on them. If you are uncertain, rather delete the email. Most companies block these spam emails.
- Check for spelling mistakes.
- Analyse the salutation. For example, "**valued customer**", a legitimate business would use your name.
- Beware of urgent or threatening language. This is usually a sign to stop.
- 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 get individuals to reveal personal information, such as passwords and credit card numbers).

Never give out your personal information!

If you receive an E-mail, SMS, Whatsapp or phone call that requests personal information such as your bank pin number, stop the call, even if the person says that they work for your Bank. Rather call the Bank and verify this.

Be weary of marketing tactics that require your personal details and state that you have won money or inherited money from a distant uncle for example. If you did not play the lottery, then do not continue with the conversation.

Usually these scams require some upfront payment and personal information. A Bank will never ask for your pin over the phone.

If you are selling something, ensure that the money is in your account first before parting with your goods/services.

Trust your gut. If it's too good to be true, then it usually is.

Be aware of scams

Pyramid schemes

- Money is raised through recruiting other people into the scheme rather than from buying or selling any product. The more people each person recruits into the scheme the more money is made by everyone who joined the scheme earlier.
- Pyramid schemes are not investments or genuine business opportunities.
- Pyramid schemes usually fall apart when it becomes impossible to get new people to 'invest'. The problems start when "recruitment" dries up and investors start losing their money.

Pyramid schemes: Be aware of this scam

How will you know if you are being scammed?

- You have been promised a lot of money back in a short space of time.
- Need to get other people to invest.
- No knowledge of where money is invested.
- Promoters are not registered anywhere.
- No way of tracing where the scheme or promoter's come from.
- Risk losing your money.
- Hardly any recourse, which means there is no one to turn to in order to get help.

Be aware of scams

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.

Ponzi schemes: Be aware of this scam

How will you know if you are being scammed?

If you are promised a high return in a short amount of time, beware. If it sounds too good to be true, then it probably is.


30

Be aware of scams

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 value of the stock price.

Investors then create a buying demand, as they believe that they are getting 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.

Pump-and-dump fraud: Be aware of this scam

How will you know if you are being scammed?

If you are approached by someone trying to sell you shares or stocks. First do your homework on the financial product.
For example:

- How long have these shares been in the market?
- What was the value of the shares in prior years?
- Is the person selling you the financial product registered with the FSCA?

Offshore Scams

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

Offshore Scams: Be aware of this scam

How will you know if you are being scammed?

If you are promised a high return in a short amount of time, beware. If it sounds too good to be true, then it probably is.


CONGRATULATIONS

Be aware of scams

Advance fee fraud

This fraud plays on an investor's hope that he or she can correct 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.

Advance fee fraud: Be aware of this scam

How will you know if you are being scammed?

If you, as an individual or your company have been:

- Promised funds, by someone you have never heard of, in return for assisting someone to transfer millions of dollars;
- Advised that you are the beneficiary of a multi-million dollar inheritance;
- Advised that you are the winner of a lottery even though you have never bought a ticket;
- Offered a fantastic business opportunity;
- Offered a confidential business proposal; or
- Offered an unsecured loan

You will be asked to pay a fee in advance for this service. Needless to say, if you do pay this fee, you may never be able to get it back.

SMS phishing

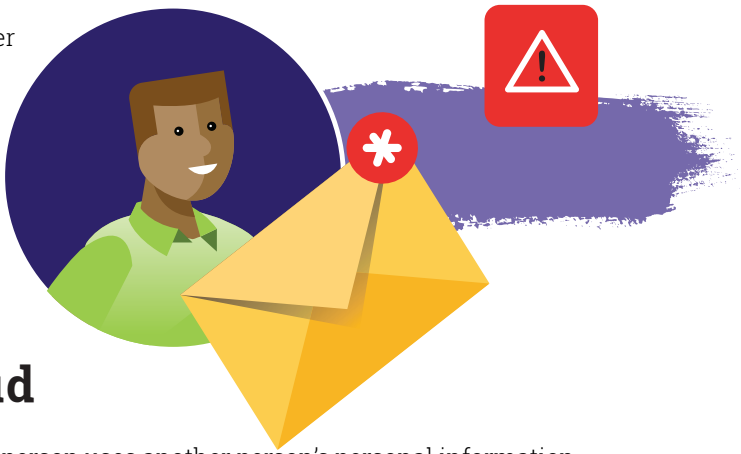
SMS phishing or smishing is a form of criminal activity. This scam makes use of lying techniques to convince you to get your personal information such as passwords and details . Fraudsters get you to send them these details by winning your trust through verious ways over email or SMS.

SMS phishing: Be aware of this scam

How will you know if you are being scammed?

You will need to give out personal information that legitimate businesses would never ask you for, such as your:
Address

- Place of work
- Bank account number
- Pin number



Identity fraud

Identity fraud is when one person uses another person's personal information, without them knowing, in order to commit a crime or to deceive or defraud that person.

Identity fraud: Be aware of this scam

How will you know if you are being scammed?

You will need to give out personal information that legitimate businesses would never ask you for, such as your ID number, bank account details, Pin number etc.
For example, the fraudster opens an account using your ID number and buys clothes on the account.

Be aware of scams

Online gift

Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores. They may use clever 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 get the item you paid for, but it will be fake, of bad quality, smaller or larger than expected or you may never get the goods that you ordered online.

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 at reasonably good prices.

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. Search for reviews online from other people who have made purchases from this store. Usually if it is a scam, many people will use the Internet to post a complaint or warning to others.

Online gift: Be aware of this scam

How will you know if you are being scammed?

- A product that sounds too good to be true.
- Need to pay upfront to get access to the gift.
- 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.
- Little or no 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.

Be aware of scams

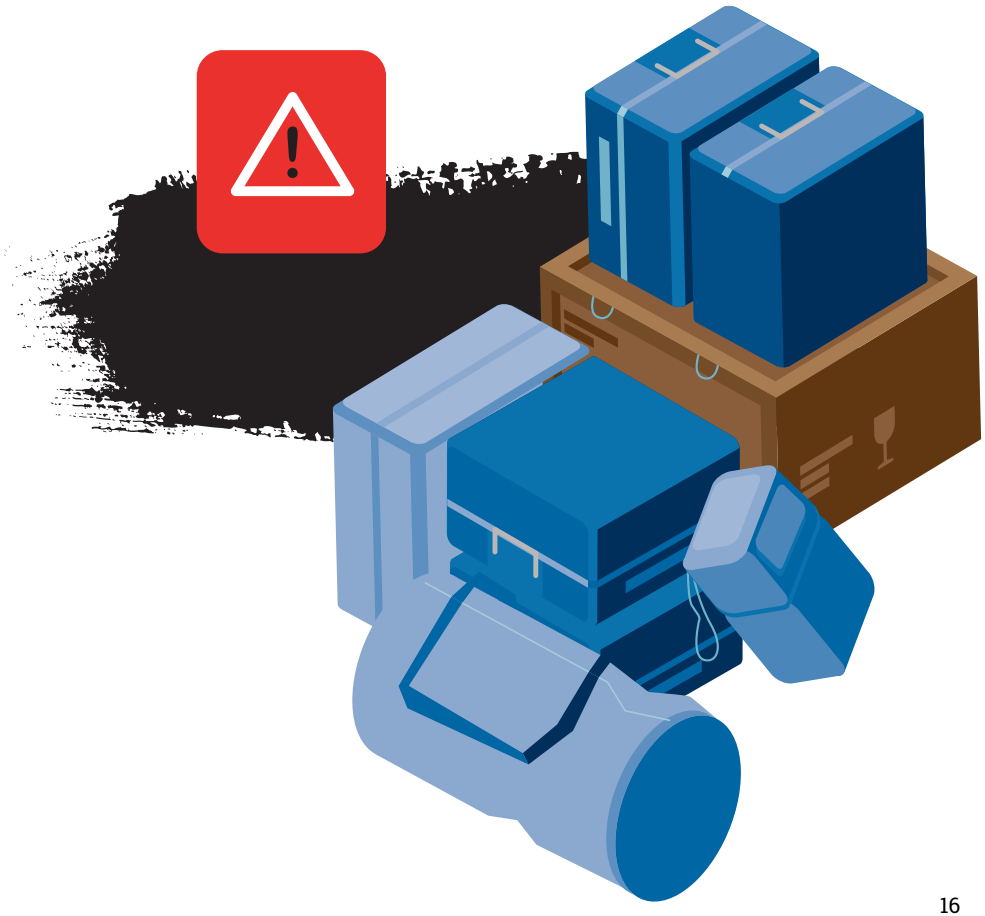
Travel fraud

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.

Travel fraud: Be aware of this scam

How will you know if you are being scammed?

- A holiday is never "free" if you have to pay something.
- No clear understanding of what exactly is included in the package.
- You need to make reservations through a specific company and the costs are higher than they would be if you used your own travel agent or made the arrangements yourself.
- The offer may be valid only if you bring a companion along at the full rate per person.
- There may be restrictions such as, deals are only available for off-peak times, not during school vacations, holidays or other popular travel dates.
- You can't find any information about this deal if you research it.
- Must pay everything upfront.



Be aware of scams

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 that you are getting a job. The conversation would normally require you to pay a fee to get the job.

Job Scam: Be aware of the scam

How will you know if you are being scammed?

- 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 capital letters and inconsistency with the use of colour of the fonts.
- Online interviews – Interviews using instant messaging service.
- Emails do not include contact details.
- You are asked to pay a fee for the job. The fee is usually not to a registered bank account, it could be a cash less transaction, cash send, e-wallet, etc.
- You are required to give out all your personal information like bank details.
- A possible job asks you for an upfront payment to guarantee you the job but you have never applied for that job or you have never heard of that company.

Be aware of scams

Truck Scam

An advert is placed for a truck and trailer but the advertiser does not have a truck and trailer. The seller never speaks to the interested buyers on the phone, only email.

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.

Truck Scam: Be aware of this scam

How will you know if you are being scammed?

- You have to pay a deposit before you get to see the truck and trailer.
- There are small details such as spelling mistakes, lack of website addresses, physical addresses and a VAT number on the invoice. There might be an email address only and no contact number.

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

Property Scam: Be aware of the scam

How will you know if you are being scammed?

When renting or purchasing a property keep note of the following:

- Be wary of upfront payment requests
- Prices too good to be true
- The email from the agent or potential buyer contains a lot of mistakes
- The agent won't show you the property
- The seller pushes you
- The seller asks you to EFT money
- The buyer or seller is foreign and wants to buy a home that he has never seen
- Know market-related prices as this is a warning or precaution for the seller or buyer
- Always question a 'bargain'
- Don't be rushed
- Always view the property before paying

More information on scams

For more information on various types of scams and schemes, visit the following websites:

https://www.sabric.co.za

http://www.saps.gov.za

http://www.scamwarners.com

http://www.419scam.org

http://www.crimes-of-persuasion.com

http://www.fbi.gov/scams-and-safety/common-fraud-schemes

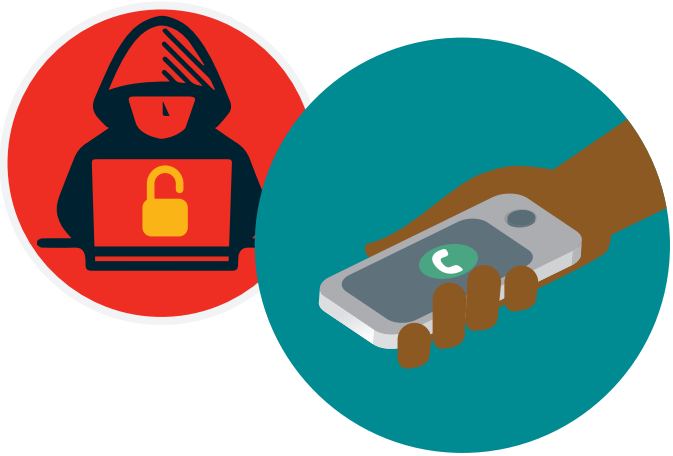
http://www.reservebank.co.za

Be aware of possible scams

Signs of a scam

There are a number of red flags that will help you identify a scam, such as:

- The deal is too good to be true, a real bargain/very cheap and the sales person is very convincing.
- There is pressure from the salesperson to sign or pay as soon as possible or you will lose out on the deal.
- No one can guarantee your return on an investment
- You are approached by a person who wants to sell you a financial product but they cannot provide you with their FSCA registration number or the relevant qualifications that authorised him/her to sell you those products.
- There is no paper trail. No documentation when taking the deal.
- Winning the lottery overseas and you have never played the lotto



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 that the investment company you are dealing with is authorised to sell you certain financial products, before parting with your hard-earned cash.

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

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

Report scams and fraud

You can check if you have been targeted by calling

Tel: 080 033 3437
email: report@easycomeeasygo.co.za
web: www.easycomeeasygo.co.za

It is our duty as South Africans to report on scams so that we can warn other people before they lose their hard earned money.

You can also use social media platforms to report scams.

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

Notes

FSCA
MyMoney
Learning Series

Scams

> The purpose of this booklet is to help you to avoid being caught by a scam. This booklet will make you aware of how easy it is to identify a scam if you know what you are looking for.

FSCA
Financial Sector
Conduct Authority

Disclaimer

The information contained in this information booklet has been provided by the Financial Sector Conduct Authority (FSCA) for information purposes only. This information does not constitute legal, professional or financial advice. While every care has been taken to ensure that the content is useful and accurate, the FSCA gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Except where otherwise stated, the copyright of all the information is owned by the FSCA. No part of this information booklet may be reproduced or transmitted or reused or made available in any manner or any media, unless the prior written consent has been obtained from the Financial Sector Conduct Authority's Office of General Counsel.

FSCA Contact Details

Riverwalk Office Park, 41 Matroosberg Road, Ashlea Gardens, Extension 6, 0181, Pretoria, South Africa | 012 428 8000 |
Share call number: 0800 20 FSCA (3722) | info@fsca.co.za | www.fsca.co.za