Hi Everyone, the following article was retrieved from https://www.moneyadviceservice.org.uk/en/articles/beginners-guide-to-scams

What it does is demonstrate to you and I how prevalent sin is when we are dealing with money. It seems there are a great number of people who spend all their free time thinking up ways to separate me from my money. And they spend all of their working time doing so to thousands of people.

Here is the beginning of an article on Geektime.com (are they reliable? I am not sure, but the site appears to be reliable.)

Smart people are easier to scam, according to a new report released by Ultrascan AGI, which recently released a report on Nigerian 419 Advance Fee Fraud statistics. According to the report, losses from Nigerian scams totaled $12.7 billion in 2013.

We have all gotten that email. You know the one, saying you just received a big inheritance, or maybe you won the lottery even though you never bought a ticket, or maybe the email sender needs to smuggle money into the U.S. and promises to give you a portion of the money in return for just a little help. If these emails even make it into your inbox instead of your spam folder, hopefully you recognize the scam, but according to the report, millions of people have fallen for these tricks, leaving huge holes in their pockets and making hundreds of thousands of Nigerians rich.

This month Ultrascan released statistics on how many victims fell for Nigerian 419 Advance Fee Fraud scams. According to the report, there are more than 800,000 organized perpetrators globally, many coming from Nigeria, and that number is growing by 5% annually. The scam is called a Nigerian 419 scam because the method originated in Nigeria and 419 is the number of the article in the Nigerian Criminal Code dealing with fraud. To be considered a Nigerian 419 scam, the perpetrator does not need to be in Nigeria, but does need to have a West African connection and must require some advance fees. According to the report, roughly 85,000 of perpetrators come from the “Nigerian Diaspora” residing in 69 different countries.

So with that in mind, I offer you the article that details some of the many scams that are ready to separate us from our money. Please, remember that as God’s steward, you are responsible before the face of God for what you do with the money in your account AND in the ministry account.

A beginner’s guide to scams

Knowing about the common scams that fraudsters are trying to use to steal your money can stop you being conned. Read these handy pointers to help you spot a scam.

How to spot a scam

There are some general signs that should set alarm bells ringing wherever you see them. Be very suspicious if:

- Something sounds too good to be true – like free stuff or quick, easy money
- You’re asked to give out personal or bank account information
- You aren’t given long to make a decision or you feel pressured into making one immediately
- You’re contacted unexpectedly by a company or person you have never heard of – this can be by post, email, phone, text or on the doorstep
- You’re asked to pay anything up-front
- The only contact details are a mobile phone number and a PO box address

Common scams and what to watch out for

Phishing

Phishing is where someone tries to con you into revealing personal information like your bank account details.

A common trick is to send you **a fake email pretending to be from your bank** or another organization you trust such as HM Revenue & Customs or PayPal, asking you to visit a website and log in with your account details. The site looks just like your bank's website, but is really a fake site set up by criminals to get your details.

Email is the most common way of doing this, but you might be targeted by text message or by phone. If you're suspicious, ask to call them back and see if the number matches your bank's real phone number. Make sure you get a dial tone before you call, in case the scammer has stayed on the line.

Pharming

This is when hackers re-direct the traffic from a genuine website to another, such as a fake e-commerce or banking site.

This is a very sneaky kind of attack as although you've entered the correct information to the right site, you're still sent to a fake one to try to get your personal information.

Advance-fee fraud

This is also known as the '419 fraud' or 'Nigerian bank scam'.

You'll receive emails from people claiming to be ex-ministers or royalty from other nations, often in Africa, asking if they can use your bank account to deposit a large sum of money in order to get it out of the country. They will normally offer to pay you a fee.

They'll ask for your bank details and may also ask you to send money to cover legal fees and so on. But there is no money and you'll be out of pocket. There is also a similar scam coming from China that's related to wills.

Dating fraud

Some fraudsters will connect with you on a dating website. They'll be up-front about living overseas and will email you, getting to know you over time and becoming affectionate and romantic.

Then once you've become involved they will start asking for money for a sick relative or for a plane ticket to come and visit – and will happily take your money but never appear.

Money Mules

Here you could unknowingly end up breaking the law and helping criminals by using your bank account to take delivery of, and then forward, stolen money and be paid a commission for helping. You would be breaking the law by money laundering.

Boiler rooms

Also called ‘pump and dump’, this is a scam where fake stock market traders contact you out of the blue and give you the hard sell on buying shares that are either non-existent or virtually worthless.

You might be offered secret stock tips to make it all seem more believable and sent fake share certificates to try to make the business seem legitimate. Then the fraudsters will disappear with your money.

Vehicle fraud

There are a number of scams around buying and selling cars.

You may be sold a stolen vehicle or a cloned car where the details of the car have been changed to match a legitimate vehicle. You could pay for a car that is never delivered to you or one that doesn’t match what you’ve paid for.

Online auction fraud

With the growth of online auction sites, there are con artists who will pose as fake buyers who appear to pay for the goods that you then send to them.

The problem is that the payment bounces. Or there could be fake sellers who take your money but don’t send the goods, or send something that’s less valuable or very different from the description.

Job scams

There are a variety of job scams which range from promises of a new career, where you're asked to pay up front for training or materials, to being offered non-existent jobs abroad where you are then asked to pay a fee to organise visas and accommodation.

You might also get caught by a **work at home scheme** where you are told you'll make easy money and you may have to pay a fee up front to register. However, the 'leads' or products turn out to be worthless and – worse still – your registration details may be sold on to other scammers.

Health scams

If you see an email or an advert for a 'miracle cure' for baldness, cancer, impotence, acne or weight loss, then steer clear.

- You could be offered something that appears to be a legitimate alternative medicine but doesn't actually work
- Or you might think you are getting drugs and medicines very cheaply or without a prescription but they may not be the real thing – if they actually turn up at all

In some cases these fake medicines can actually damage your health.

Prize draws, sweepstakes and lottery scams

You could get a letter or email telling you that you have won a lottery, sweepstake or other prize draw and offering you a large prize. The scam can then take different forms:

- You might be asked to send a small amount of money in order to claim it as a processing fee or legal fee – but no prize exists and you lose the cash
- You might be asked to prove your identity with a passport – which is then used by the crooks to steal your identity
- You might be asked to provide your bank account details so they can pay the money in but this information is then used to clear out your account

- You might be told you have won a prize and you need to ring a special phone number to claim it - the call goes to a premium rate number, takes ages and will cost you more than the value of the prize you've won

Property fraud

If someone offers you a get rich quick property scheme then there are a variety of ways they could be trying to defraud you.

- You might be offered a way to buy into a development that is not yet built with all sorts of claims about the profits you'll make – but the land is either farmland or derelict and will never get planning permission or is unsuitable for development so you'll lose your money. This type of fraud is also sometimes called 'landbanking'
- A fraudster might steal the title deeds to a property and pretend to be the owner and then try to borrow money against the property

Face-to-face fraud

There are many legitimate door-to-door sales staff – but others don't have good intentions. You can be pressured into buying something you don't want or isn't worth the money you pay for it.

Fraud by bogus tradespeople can take a variety of forms:

- Fake charity collections
- Selling you unfair or unsuitable contracts
- Home maintenance or improvements that you are overcharged for or are badly done
- Potential thieves who are checking out your valuables once inside your home

Pension scams

Pension fraudsters will tell you they know a loophole so that you can get hold of some of your pension money before retirement. While you can make arrangements to get cash from it if you're 55 or over, **it's likely to be a scam** if you see claims that:

- **You can get cash before the age of 55**
- You can get **more cash than under your current scheme**, or
- You can have **more than 25% of the pension value "released"**

They might charge you a fee or land you with a big tax bill.

Next steps

There are numerous ways to be parted from your money. Check out more potential fraud situations so you know what to avoid.

How to avoid being scammed

Given the number of potential scams there are easy ways to make sure you don't become a victim.

Protecting yourself from scams and theft

There are many con artists out there trying to part you from your money. Follow these tips to prevent yourself from becoming a victim of fraud.

How to recognize a scam

These days most people know about dodgy emails that try to get them to hand over their personal details or buy knock-off prescription drugs or watches – and the biggest risk of fraud is still online. But you can also fall prey to the tricksters by phone, by text, by post and in person.

The best advice is that if something seems too good to be true – it usually is.

Top tips for protecting yourself from scams and theft:

Taking some simple steps will make sure you are better protected:

Keep your cards and PIN safe and secure

- Make sure your cards and PIN are safe – don't write your PIN down, and if you have, make sure you don't keep the note and your card together.
- Don't let your card out of your sight when you're paying.
- Don't give your PIN to anyone else.
- Shield your PIN whenever you enter it – both at a cashpoint and whenever you use your card for a purchase.

Make sure your computer is protected, and use it wisely

- Keep your security software and firewall up-to-date to find viruses, spyware and other 'nasties'.
- Download any patches for your computer's operating system from the official website of the company that created it (like Microsoft), as some fraudsters target possible loopholes. Patches fix known bugs for computer systems.
- Password-protect your computer with a strong and not easily guessable password and make sure your screen's locked when you're not around. For a strong password, use a mix of letters and numbers – this can still be easy to remember if you use numbers to represent letters in a word.
- Bookmark websites like your bank and the shops you buy from regularly, and use these links or type in the name directly. Never use links sent to you in emails they might be bogus, even if they look genuine.
- Don't give your online passwords away. Banks generally won't ask for a full password – just selected letters from it. If someone rings you up and asks you for your full password don't give it to them – it's likely to be a scam.

Be a sensible online shopper

- Check the details of a company you are buying from online. If the only contact details are a mobile number and a PO Box rather than a full address you should be wary.

- Make sure that the website is secure. **Only provide card details if the web address starts with https://**. Often a golden padlock will show in the browser bar so you know it's safe and secure – although some companies use a different system and their sites will be secure even with no padlock.
- Sign up to Verified by Visa or MasterCard Secure Code if you have the option while shopping online. It provides an extra layer of security for you with shops that have signed up to the schemes.
- Deliberately enter a wrong password – you can check a site is genuine if you enter your user name and put in a wrong password. If the site is genuine it will tell you that your user name and password don't match.

Check the credentials of any financial adviser you use

The Financial Conduct Authority (FCA) requires all firms offering financial products or advice to be registered with them to conduct business. You can use their online firm check service if you're unsure about a firm that has contacted you.

Keep your details safe

- Shred any documents you're getting rid of before binning them if they have any personal details on them.
- Don't forget to shred receipts if they have your card details on them.
- Get a shredder now if you haven't got one – you can pick one up for less than £20. Although do consider a cross-shredder as these are more secure than the 'strip-cut' variety.
- Keep all documents that you still need in a safe place.

Stay alert and be suspicious

- Ask people for ID if they approach you or knock on your door.
- Think twice if either you get an unsolicited offer, you've been told you have won a prize in a competition you haven't entered, or you're being pressured to decide on buying something quickly.
- Check and double check before handing over any money or personal details.
- Check your bank statement when it arrives and query anything that seems odd.

What to do if you think someone is trying to scam you

If you receive an email you suspect to be from a scammer – don't open or reply to it, don't click on anything in it, or you'll just end up receiving more. If the email you are suspicious about is pretending to be from for example your bank, it's worth contacting the bank and telling them about it. They may then be able to warn other customers. If you have the option to report the email to your email provider, use it.

- Don't reply to suspicious letters received in the post. Signing up to the Mailing Preference Service should help stop any further unsolicited mail. It's free, and you can do it at mpsonline.
- Similarly, signing up to the Telephone Preference Service makes it illegal for companies or organizations who want your business to call without your permission. Sign up for tpsonline.
- You can report the scams to Citizens Advice consumer service and you should report banking scams to Bank Safe Online.
- If you're called by a scammer then hang up the phone, and don't give out any personal details.
- If someone asks you to keep the deal or the offer secret then you should be suspicious of them and decline the offer.
- If you suspect someone isn't from the company they say they work for, then ask to see their ID (in the case of a face-to-face scam).