BECOME CYBERSAFE AND LEARN HOW TO KEEP YOUR PERSONAL INFORMATION SAFE.

Cybercrimes such as fraud, phishing and scams are an everyday reality and it's important to stay informed and be alert to prevent yourself from becoming a victim.

We've put together a useful guide to help you stay safe online.

USEFUL TIPS TO HELP KEEP YOU SAFE ONLINE

Phishing

How to spot an unsafe link

Scams

Report a scam or fraud

REPORT A SCAM OR FRAUD

We encourage our staff, clients and stakeholders to report unethical or corrupt behaviour. If you suspect fraudulent activity involving any of X'S Sure's insurers or clients, you can confidentially report this.

PHISHING

When is a message FAKE?

Phishing is when you are contacted out of the blue (without you requesting it) and are requested to provide personal information, participate is some activity, open an attachment or simply just click on a link. This can happen on email, WhatsApp, SMS, Facebook, LinkedIn or even over a phone call. The golden rule is to always think before you respond and never provide personal information including user IDs and passwords.

HOW TO SPOT AN UNSAFE LINK

Knowing the difference between a safe and unsafe link can help you stay safe online.

Don't trust any link or attachments in emails or social media messages you were not expecting.

Always hover over links in emails to see the actual link.

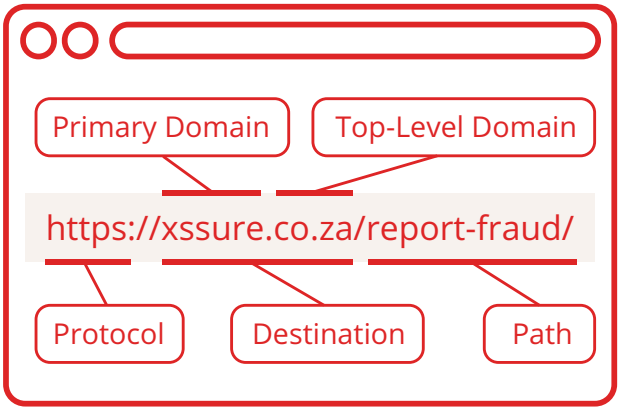
If you understand the anatomy of a URL, you will be able to see the primary domain, which is the important part of a URL as it tells you where the link will take you if you click on it.

For example, in the X'S Sure URL: **https://xssure.co.za/**, the destination is xssure.co.za. In the URL: **https://google.google-fake.com**, the destination is google-fake.com or in the URL: **https://verify.microsft.really.com/microsoft.com** the destination is really.com and NOT microsoft.com.

To identify the destination that a URL is going to take you to, look at the part AFTER the https://. Now start before the first slash "/", or if there is no slash start at the end of the URL and look at the parts before that point. The destination is the TWO last parts if the top level domain is .com or the THREE last parts if the top level domain is .co.za.

The diagram below shows you that the destination is the primary domain and the top level domain together.

Anatomy of a URL



When visiting websites, the safest methods are to create bookmarks or manually type in web addresses. Making use of reputable search engines is the next best option, but you still have to apply the "anatomy rule".

SCAMS

The COVID-19 pandemic spurred a major increase of opportunistic criminal activity on the internet.

Cyber criminals are sending all sorts of scams related to the pandemic. Malicious websites and phishing attacks are benefitting from the COVID-19 panic, and are targeting people working from home, many of whom face dire financial situations. Scammers are setting up fake charities, advertising fake COVID-19 related products, spreading fake news and luring us with low interest loans or high return investments.

The objectives of these attempts are to steal your money and/or access your personal information.

Spotting a Scam

Be wary when you see:

- Any message (email, SMS or WhatsApp) trying to persuade you to transfer money to a beneficiary account number that is new or unfamiliar to you
- An upfront request for advanced payment
- Communication containing linguistic and grammatical errors (but not always)
- Guaranteed high or quick returns – any 'get rich quick' promises
- An email address which you're unsure about or doesn't look exactly right
- Any message which tries to pressure you to make a decision and act

Don't be fooled into thinking that:

- Scammers will not use WhatsApp, because you can see their cell phone number
- The scammers have a true concern for you as a person
- Scammers will not try to use reputable brands like that of X'S Sure.

Responding to Scams

If it sounds too good to be true, it is too good to be true. Be very cautious of highly lucrative investment offers.

- If anyone contacts you or if you receive an unexpected and unfamiliar message on email, SMS, WhatsApp, Facebook or LinkedIn, don't respond. DON'T click on a link, open an attachment or provide any personal information.
- Whenever you receive a link, don't simply click on it. Rather visit the "real" website by doing a Google search or type the website name to check its authenticity.
- Don't trust anything you didn't expect, even if it looks like it comes from someone you know or trust. Verify the offer by using an alternative channel and alternative information.
- If you need help or want to report a scam, call X'S Sure Client Care Centre on 08600 181 40

Examples of Scams

Watch out for these known scams trying to impersonate the X'S Sure brand.

Vault Account Scam

International sources have informed us about a scam that is very effective with older people. The fraudsters contact the victim, presenting themselves as the fraud department at the victim's bank. They inform the victim that fraudulent activity was detected on their bank account and suggest that the victim transfers the money from their account to a 'Vault Account' for safekeeping, while the bank "investigates the attempted fraud". The 'Vault Account' is owned by the fraudsters and the victim loses the money.

Fake Investment Schemes Scam

Be aware of recent scams that impersonate the X'S Sure Brand and target potential customers via Facebook or WhatsApp.

Fraudsters have shifted their focus to WhatsApp, Facebook or SMS because users are now more vulnerable to scams on mobile phones, as people find themselves being more distracted and often don't apply the same vigilance on their phones as they would on their computers. The scams are quite focused and conversational, which creates trust, so please ensure that you always verify all messages received.

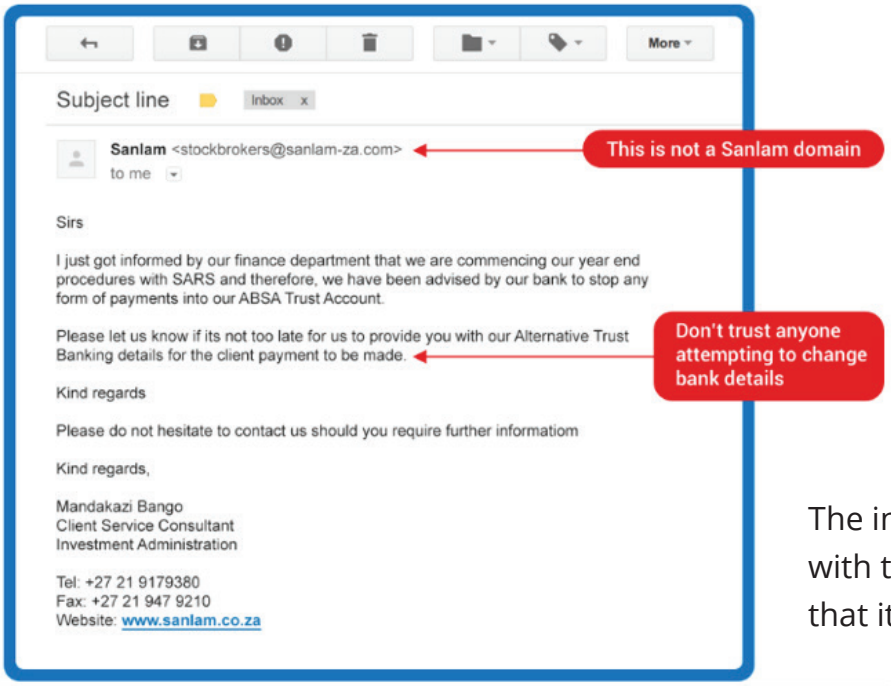
How does this attack work?

1. You receive a message via Facebook or WhatsApp, advertising a fake X'S Sure investment product. The returns of these investments are too good to be true, but to the uninformed investor, this looks like a very good opportunity.
2. The fraudsters often use names of X'S Sure senior management, as well as X'S Sure branding and even provide X'S Sure brochures. The fraudsters source all this information from public platforms, like internet websites.
3. Victims who fall for this are then asked to join a X'S Sure branded business WhatsApp group and are instructed to pay the investment amount into a nominated bank account and provide proof of payment.
4. Once payment is done, the victim can no longer gain access to the WhatsApp group and usually ends up calling X'S Sure.

What to watch out for:

1. Any random messages (email, SMS or WhatsApp) trying to persuade you to transfer money to a beneficiary account number that you have not dealt with before.
2. If the offer sounds too good to be true, it usually is (fraudsters pry on emotions like fear and greed).
3. When receiving anything unexpected, always say to yourself: "Stop – Think – Verify". You can also contact X'S Sure to verify.
4. If you have fallen prey to such a scam, report it immediately to X'S Sure.

Change of Bank Account Details Scam



The information highlighted with the red flags indicates that it is fake.

Hacked Email Account Scam

This is an attack that shows the value of keeping your email account safe:

Someone manages to hack into your email account by guessing your password or tricking you into handing over your password by a cleverly crafted phishing email.

When logged into your email account, the fraudster sends X'S Sure fraudulent instructions and deletes all of these emails without your knowledge. They can potentially also use your email account to reset passwords for other services you might be using that allows such changes. Should these sites not send alerting messages to your cellphone, you will not know about this.

This is a common fraud pattern and very dangerous as you may not even be aware of it happening. Due to this risk, X'S Sure doesn't accept high risk instructions by email only and will confirm such instructions with a phone call.

FRAUD REPORTING

X'S Sure is committed to the highest standards of business integrity, ethical values and governance.

We encourage our staff, clients and stakeholders to report unethical or corrupt behaviour. If you suspect fraudulent activity involving any of X'S Sure's partners or clients, you can confidentially report this.

Anonymous
Report fraud anonymously.

Confidential
Report fraud confidentially.

View FAQ
View the Frequently Asked Questions.

Report Online
Report fraud using our online form.

Anonymous Reporting

Our Fraud and Ethics Hotline is managed by an external provider, which guarantees the anonymity of the person wishing to report fraud or unlawful conduct anonymously. The identity of the person making the report will not be disclosed to X'S Sure. Therefore, you do not need to supply your identity or any information that may reveal your identity. By selecting this option, it means that we cannot contact you for more information if needed.

T 08600 181 40 **E** leon@xssure.co.za

Making reports with malicious intentions are strongly discouraged

Confidential Reporting

By completing the online reporting form, your identity will be known to the investigator who may contact you for further information if needed.

Before submitting the reporting form, please familiarise yourself with the contents of the privacy disclaimer.