Security and fraud

Ethics Hotline

We are serious about preventing fraud and misconduct in the Guardrisk

environment. If you suspect fraud, irregular or unethical practices, you can report

it by contacting:

Telephone: 0800 000 484
Email: guardrisk@tip-offs.com

This service is provided and administered by Deloitte Tip-offs Anonymous (Pty), which ensures an independent and unbiased reporting platform.

All incidents reported will be handled with the strictest of confidence, and the caller's identity will remain anonymous.

We view any criminal activity as an extremely serious matter with zero-tolerance for misconduct or fraud and are committed to the enforcement of an anti-crime culture throughout the organisation.

Reporting directly to Momentum Group Limited Forensic Services – Ethics Helpline

Reports can also be made directly to the Group Forensic Services department of our parent company, Momentum Group Limited. All direct disclosures will remain confidential and that every effort will be made not to reveal the identity of an informant.
Email: dlotter@mmltd.co.za

Online scam alert
Scammers are running fake social media profiles and bogus websites. They lure individuals in with a promise of low repayment loans or high returns on investments in a short space of time. These scammers may also go to great lengths such as creating websites with an error in the domain that may not be noticed at first sight, domains such as www.gaurdrisk.co.za (incorrect spelling of Guardrisk).

We would like to assure you that none of our staff will approach you in this manner, nor would they require of you to opt into any of our services and products through a social networking site or pay money into an account without a valid contract/policy in place. Furthermore, our staff are not authorised to accept cash or deposits into private bank accounts on behalf of Guardrisk. Please be vigilant on any of the tricks that the scammers may present.

If you need clarity on this or would like to authenticate a message, feel free to send us a mail at info@guardrisk.co.za – we endeavour to respond to all emails within 24 hours. Whilst we may ask for additional information, this is for your protection.

Protect yourself from fraud
Your security is a high priority for us, especially as we see an unprecedented increase in fraudulent activity. Scammers are getting very clever in deceiving people, but we can defeat them together if we are extra vigilant, aware, and cautious. We've listed below a few of the common scams our experts have identified.

Financial scams
Scammers pretend to be from reputable companies. They either create fake social media or WhatsApp posts and profiles to convince you to share your personal or financial information – often with promises of exorbitant or unrealistic financial returns or large sums of money for little or no effort on your part.
The profiles often impersonate actual employees or use a real company's name or logo. Always think twice before handing over or depositing money or providing your information to the suspected scammer, as it can be used to access your bank account, make fraudulent purchases, or steal your identity. Once you've deposited your money into the bank account nominated by the perpetrator, you'll likely never hear from them again.

Employment scams
Legitimate employers will never promise work in exchange for an up-front fee or favours. There's also no good reason for you to send them your bank account details before securing a job.

Do not go for interviews in unsafe places. Reputable companies will interview you at their offices or a registered employment agency or via an online call. Never agree to meet someone at a private home or apartment for an interview.

Things to look out for
Criminals come up with new ways to steal your money and identity every day. Here are a few things you can look out for to ensure your safety.

- Black laptop keypad with white letters and a red trackpoint.
- Emails asking you to confirm personal information, such as passwords, personal pins or your ID number. This one should always be a huge red flag.
- “Business” emails sent from public email domains. Another red flag.
- Emails using generic greetings such as “Dear Sir” or “Hello dear” instead of your name.
- Unexpected emails from unknown or even legitimate-looking sources, prompting you to click on a link or attachment.
- Poorly worded emails. Pay as much attention to grammar as you would the spelling.
- Always check that the URL provided matches the actual domain.

Types of phishing scams
Find out about popular phishing techniques, to help keep you clued up, and armed with enough “tech-savvy” to avoid getting scammed.

Deceptive phishing
This is by far the most popular method used by fraudsters. You get a credible-looking email from a bank or other reputable institution asking you to confirm personal information either by responding to the email or following a link. No reputable financial institution will ever ask you to disclose sensitive information through an email, SMS or digital link.

Link manipulation and smishing
Crafty and often difficult to spot. With this technique, you receive a link and click on it, thinking it’s taking you to a specific website, but you land on the phisher’s malicious site, which is often a duplicate of a legitimate website. Always be wary of emails prompting you to click on links or attachments.

Spear phishing
Unlike traditional email phishing, where one email is sent to numerous random users, spear phishing is more targeted. Fraudsters study their victims' online habits then customise their messages accordingly. When you open the email, the source and content look legitimate, and the next thing you know, you've been scammed.

Vishing
Vishing is merely phishing done through a telephone call. Similar to the electronic version, the aim is to trick you into handing over confidential information to the caller, who usually claims to be representing a legitimate institution such as your Insurer or Bank.

Website spoofing or forgery
As the name suggests, criminals create a replica of a genuine website, with the aim of collecting confidential information from users in order to defraud them. Always check to see if the URL is correct and matches the website. Preferably type the URL yourself rather than follow a link.

Tips to stay safe online

- ***Don't share personal or financial information*** – Don't share details of your financial circumstances or any other personal information prior to verifying that the information was requested by an authorised representative of a financial services provider. Legitimate companies will not call, email, SMS or WhatsApp to ask for your personal information.
- ***Learn to identify possible scammers, phishing emails, and malicious websites*** - Scammers may change one letter in a legitimate email address or use fake websites, or fake social media accounts and WhatsApp profiles to defraud you. Their objective is purely to access your personal accounts, such as email accounts, bank- and other financial accounts.
- ***Know who you are transacting with*** – Guardrisk employees will never ask you to deposit money into differently named or personal bank accounts or to make payments via WhatsApp. If you receive a call or email from someone claiming to be from Guardrisk, first contact us directly to verify that the person is genuine.
- ***Never deposit money into personal bank accounts*** – Always check that lump sum payments, any money or premiums are going directly to the company (eg insurer, broker, intermediary, etc) and not to individuals or personal bank accounts.
- ***Be careful what you share*** – Beware of unsuspected attempts to get your personal information, like filling out application forms, answering phone surveys or responding to social media quizzes. Don't fill out every field on your social media profile such as your phone number, home address or company details – including these details significantly increases the chance of identity theft.
- ***Stranger danger*** – Beware of direct messages or friend requests from people you don't recognise or can associate with known friends of yours.
- ***Get rich schemes are just that, schemes*** – Beware of unrealistic promises of low repayment loans and high financial returns over a short period of time. If an offer looks suspicious or too good to be true, it usually is.
- ***Don't be pressured in deciding on the spot*** – Offers that are time sensitive or urgent are usually scams. Legitimate organisations will give you time to make an informed decision, so don't be pressured into making decisions immediately.
- ***Interception of e-mails is increasing*** – When someone clicks on a phishing link, a link that looks identical to the legitimate address, the criminal can gain access to your email account, upload malware to your machine or take over your machine. Tip: Hover over the link with your mouse (but don't click on it) to confirm the email address or website is legitimate. It is highly recommended to change your email account settings to enable multi-factor authentication. Constantly review and improve the strength of your passwords. Password123 is not a good password! And DO NOT use the same password for all your online activity. Create complicated passwords, consisting of capital letters, numerical numbers and special characters that are not easy to decipher and remember to change them often.
- ***If anything feels wrong, stop, and check what you are doing*** – Check every detail and every spelling, contact the company directly to check if it is them that you are doing business with. Especially check bank deposit details and never hand over cash or deposit money into an individual's account. A moment to check or one phone call can save you from being caught out.

Already been scammed?

Take immediate action to avoid further damage.

- If you are unsure about the legitimacy of an offer or would like to verify any Guardrisk employee, rather contact info@guardrisk.co.za
- If you come across a social media account impersonating a Guardrisk employee, report it to info@guardrisk.co.za.
- Report and lay a charge with the South African Police Services.
- Where identity theft is suspected, the matter must be reported to the Southern African Fraud Prevention Service at https://www.safps.org.za/
- Look out for warning signs that your information may have been compromised, such as unexpected SMSs asking you to verify your pin.
- Change **all** your passwords immediately. This goes for emails, online banking and other profiles, as well as social media passwords.
- Run a full system scan to help detect any viruses or harmful malware in your device.
- Get in touch with crucial institutions like your bank, insurance provider and retail stores you may have credit accounts with, to inform them of the fraud.
- Inform all major credit rating agencies to protect your credit record.
- Report the fraud on the Southern African Fraud Prevention Service (SAFPS) helpline: +27(0)11 867 2234.
- Visit the https://www.safps.org.za/ website for more comprehensive tips on fraud prevention and other useful contacts.