Fedgroup security notice

Introduction

Fedgroup has built our reputation on always putting the needs and interests of our clients first. We are therefore fully committed to go above and beyond the normal requirements to ensure that our clients' safety is never compromised. To achieve this, we employ the latest technology to safeguard our clients, both in terms of their investments, and against online threats that include identity theft and fraud.

Fraudulent email schemes (phishing schemes) have seen a dramatic rise in the last few years. Not only are they becoming more frequent, but they are also becoming more sophisticated. They often use letterheads and logos to look like they come from a legitimate financial services provider. Never provide any personal details or transfer any money unless you are absolutely certain that you are dealing with Fedgroup directly or through your trusted broker.

Delete any suspicious-looking email immediately and contact your service provider. Do not respond to these mails.

Our responsibility

The online security of every Fedgroup client is of paramount importance to us. All client transactions on our online portal are managed through best practice encryption and protection. All sessions are subject to automatic logouts after a period of inactivity. Multiple failed password attempts will result in automatic lockout and clients would have to verify their identity before the account is unlocked for online access.

Fedgroup's servers are protected by multi-level, enterprise-grade firewalls that guard all access points, and is tested regularly to ensure that it conforms to the latest industry safety standards.

Both our online portal and our mobile application do not allow users to change their banking details. These details can only be amended through direct contact between the client and Fedgroup, subject to positive verification. No in-app verification is enabled.

Collection of personal data
Your safety, security and privacy are of the utmost concern to us. To enable you to log into your account, we need to collect personal data to be able to identify you and to keep your account secure. This data may include:

- Name and surname
- ID number
- Physical address
- Email address
- Phone number
- Cookies

From time to time, we may use this data to get in touch with you with useful information. You can opt out of this communication at any time by unsubscribing.

Retention of data
We will only keep your data for as long as we need it to provide you with the service you require, or in line with what the law expects from us. We will not disclose this data to anyone, unless there are legal requirements that compel us to do so.

Usage data
Fedgroup keeps a database of your last login, as well as evidence of failed login and retry counts.

Location data
Fedgroup does not track your location through our website.

Tracking and Cookies data
We use cookies to store your session. This allows you to use the site without having to constantly provide your credentials. We do not use cookies to store tracking and similar information.

Your responsibility

The use of this website is at your own discretion
Fedgroup has taken every care to ensure that all information on the website is accurate. However, it should not be seen as financial or other advice and we encourage you to always consult a professionally accredited financial advisor before making any financial decision.

As such, we do not warrant that the website, calculators, services, opinions, statements or content are completely free of error. The use of such is at your own risk. We reserve the risk to amend our pages and correct any error or omission as and when they become apparent. Information such as interest rates change constantly and updating this data on every area of the site may be delayed. Again, the advice of a financial services professional is strongly advised to ensure that you make an informed decision.

While we use the latest technology to safeguard our website and our clients, we do not warrant that the website or any available downloads are completely free of viruses or destructive code, and cannot be held liable for damages arising from this.

The choice to use the website and provide personal information is always yours. However, if you limit the information provided to us, it may limit the services we are able to provide to you.

General
- If anything looks different from the normal process, contact us before proceeding.
- If any activity on your account looks suspicious, don’t wait. Contact us right away.
- Don’t click on an email link to what may look like a logon page. Always go to the Fedgroup page or App yourself.
- Although it may be more effort, it is always better to use long and complicated passwords.

- When you transact on the Fedgroup website, look for the little padlock before the web page address at the top of your screen. This will indicate that the site is secure. If you are typing in the URL, ensure that it starts with https and not just http.
- Download and install the latest antivirus software on your computer and run regular checks.
- Never use public computers or internet cafes to do your online banking.

Mobile

- Never store passwords in any text document on your phone.
- Download and install the latest antivirus software on your phone and run regular scans.
- Don't just close your Fedgroup or any other finance Apps. Always log out.
- Don't use public mobile hotspots when doing your online transactions.
- Don't leave your mobile phone, tablet or other device where you do online transactions unattended.
- When a new software version becomes available, please download and install it, as it will contain the latest security measures.
- Passwords are still the most secure means to unlock a locked screen.
- Make sure you download your App from a legitimate app store.
- If you have any financial apps on your mobile phone, please ensure that your automatic lock screen is on at all times.

Phishing

Phishing is any form of digital communication (such as emails, texts or advertisements) that tries to get your personal information by acting as a trustworthy entity. Please keep the following safety information in mind to safeguard your details against phishing attacks:

- Never reply directly to emails asking for your personal information.
- We already have the personal information of all our clients. We won't ever send you communication asking for it again.
- Always type the Fedgroup address into the address bar. Never follow a link.
- Always delete emails that look like spam and rather call us directly. Even if you respond to a fraudulent-looking email by asking to be removed from the mailing list, you are confirming that your account is active, which is often the first step that criminals use in a phishing attack.
- Be sure that you trust a source before you open any attachment.
- Ensure that your browser is up to date with notifications that alert you when you go to a potentially unsafe web page.
- Look at the source of the email. If it comes from a free email service such as Gmail, Yahoo or Hotmail, and not from the financial services provider, it is probably a scam.
- Remember that phishing scams can also happen through voice calls (vishing) or texts (smishing). Never share your personal details via text messages and only do so on phone calls if you have contacted a trusted number.
- Be very wary of any request to pay money upfront, and only receive the service later.
- Financial services providers are often prohibited by law to offer cash prizes. If you receive communications from a financial services provider claiming that you have won a prize, it is probably a scam.

SIM card scams

SIM swaps
Although cell phone service providers go to great lengths to safeguard their clients, it does happen from time to time that fraudsters are able to perform an illegitimate SIM swap. When they do this, they receive all messages that are sent to you. If they get your personal information, they are able to change your details and withdraw your money into their accounts. We will therefore not allow you to make changes to your bank account details unless you contact us and verify your personal information.

Porting
Fraudsters can gain access to your mobile device by porting your number to a different service provider. Do not ignore any texts that confirm porting to another provider. Please contact your service provider and our fraud centre immediately.

Twin SIM
If you have not twinned your SIM card and you receive messages from your mobile service provider about twin SIM functionality, please contact your service provider and our fraud centre immediately.

Physical security

- Store away all physical personal and financial documents in a safe place.
- Never carry sensitive information in your wallet or purse unless absolutely necessary.
- If your wallet or purse is stolen, contact all your service providers and cancel all your cards immediately.
- Shred or destroy any sensitive documents or old cards before you throw them away.

Report any issues as soon as possible

If you have any suspicion that you may be the victim of online fraud or identity theft, or that someone may be trying to access your accounts or information, please do not hesitate to get in touch with us at the details below:

Tel: 011 065 065
Email: mlco@fedgroup.co.za