

# Be Cybersmart

## 'Change of Bank Account' Scam

We have noticed an increase in the amount of "change bank account" attacks within the industry. Although this is quite an old scam, criminals are making their schemes more believable and sophisticated to the point that victims have suffered financial losses.

### How it works:

1. The attacker first breaks into the email account of a client or a broker. They do this through guessing the passwords or stealing credentials via phishing.
2. Once in the mailbox, they intercept any emails related to invoices or payments. They then send an email that looks similar (with some content adjusted) to request a change of bank account details for payments. Of course, these details belong to the fraudster.
3. The attackers could even go as far as registering fake domains and accounts (i.e. glacier-za.com) to spoof the address and make it look more legitimate.

### Spoofting:

*Forging the identity of a sender making you think that it is from someone you know*

### What it looks like:

The screenshot shows an email from Glacier Shares (GS) dated Tues 20/11/2018 15:22. The sender is identified as Glacier Shares <stockbrokers@glacier-za.com> with the subject 'Low Fee/Income Requests - November 2018'. The email body contains the following text:

Sirs

I just got informed by our finance department that we are commencing our year end procedures with SARS and therefore, we have been advised by our Bank to stop any form of payments into our ABSA Trust account.

Please let us know if its not too late for us to provide you with our Alternative Trust Banking details for the client payment to be made.

Kind Regards

Please do not hesitate to contact us should you require further information

Kind Regards,

**Mandlakazi Bango**  
Client Service Consultant  
Investment Administration

Tel: +  
Fax: +  
Web:

Glacier Financial Solutions (Pty) Ltd, A member of the Sanlam Group  
Reg No. 199902336007 Licensed Financial Services Provider  
Refer to the Glacier website for details of directors

Four callout boxes highlight red flags:

- The FROM address field showed a glacier-za.com domain, instead of glacier.co.za.** (Points to the sender email address)
- The font differed between the content of the email and the signature.** (Points to the signature block)
- The email instructed the recipient to contact the 'spoofed' email address to obtain the new 'Alternative Trust' Banking details, as no payments will be processed into the old Trust account.** (Points to the main body text)
- The words 'Kind regards' were repeated - in what seems to be a copy and paste error** (Points to the two 'Kind Regards' lines)

### **Make sure you don't fall for this scam:**

1. Familiarise yourself with the indicators of a phishing or fraudulent email.
2. Protect your email account by enabling multi-factor authentication. This is combining your password with something that you own, like a One Time Password (OTP) app.
3. If this is not available, use a strong (long) password or passphrase - more than 14 characters if allowed by the mail system.
4. Always be wary of changing bank account details. If a request is received, verify by calling the sender's contact details that you have on record (do not use the number provided in the fraudster's email).
5. Beware of supposedly confirmatory e-mails from almost identical e-mail addresses, such as .com instead of .co.za, or addresses that differ slightly from the genuine one e.g. by one letter that can be easily missed.
6. Warn staff with the responsibility for paying invoices about this scam.

### **Need help?**

Forward the message to [phishing@sanlam.co.za](mailto:phishing@sanlam.co.za)

