SPECIAL OPERATIONAL CIRCULAR

22 April 2020

Dear Intermediary

PROTECT YOURSELF AGAINST COVID-RELATED FRAUD AND SCAMS

The coronavirus has emerged as a primary cybercrime theme in the last few weeks as the pandemic takes hold globally. Last month we highlighted COVID-19 scams that are prevalent during these trying times.

Cybercriminals are taking advantage of the fact that people and businesses are working remotely during the lockdown period, as this creates a perfect opportunity for less security and more time online.

The top fraud categories are related to travel and vacations, online shopping, false text messages and imposter scams. In the past two weeks, there has been a significant spike in ransomware attacks and phishing scams in particular. The majority of these attacks start with SMS messages or e-mails that direct victims to domains seemingly related to COVID-19 news, governmental updates, or health-related products and services. Whatever you do, do not reply to e-mails, SMS's or WhatsApp messages offering a miracle treatment to prevent or cure COVID-19 or possible inheritances of huge sums of money.

Banking scams and fake investment cons

Exercise caution whilst transacting on banking and remote payment apps. Whilst lockdowns are in effect the increase in remote transactions puts banks' IT systems under strain – this has proved to be an opening for cybercriminals to commit fraudulent transactions. Also, exercise caution against phone scams from your "supposed" bank. These scammers, unfortunately, target the lonely and vulnerable – so please also caution elderly family or isolated family members.

Be cautious when receiving and responding to e-mails about the "change of bank account details". Remember to phone the person requesting the bank account change and validate the information telephonically.

As global interest rates drop in the wake of the COVID-19 crisis, many consumers will be looking for new investment opportunities and financial products. Fraudsters are using the pandemic to target individuals with fake investment scams, offering attractive deals that encourage you to invest.

Short-term insurance fraud

Although it is difficult to indicate how the short-term insurance industry including Santam will be impacted, you need to please be extra cautious when processing claims in the below areas.

- Accidents where the vehicle will be a complete write-off and there is no independent witnesses.
- Accidental, flood, hail, lightning and storm damage
- Power surge claims
- Loss of jewellery items
- Motor hijackings (fraudsters require income to support their vehicle instalments)
- VAS products

SPECIAL OPERATIONAL CIRCULAR

22 April 2020

- Fire claims at small commercial businesses
- Claims paid into bank accounts other that the debit order bank account

This risk is heightened by the fact that human interaction is being reduced as far as possible; inspections are being performed virtually and communication is via technology.

Domain spoofs

In the latest attacks, which have been seen globally, victims that click the affected links are directed to one domain and then immediately redirected to yet another. By pretending to be an insurance company, bank, medical expert or other trusted brand, criminals are convincing victims to trust them. Once trust is established, the criminal is betting on the victim doing as asked, by opening malicious attachments/links, and releasing sensitive personal information, to enable access to critical applications and services.

Stop the spread of fake news

As a final warning, we also ask that you play your part in preventing the spread of "fake news" by not forwarding on any messages that appear suspicious. Anyone that creates or spreads fake news about the Coronavirus/COVID-19 is liable for prosecution. Remember to always verify the information before you share.

Cybercriminals have, for months, attempted to take advantage of the coronavirus crisis by launching phishing attacks and creating coronavirus-themed malware. These scams will probably not slow down until the crisis is over, so in the meantime, we ask that you be wise to some of these scammer tricks.