MAZARS

COVID-19 Building Cyber Resilience

TERENCE GOVENDER

Director IT Advisory

MAZARS

CONTENTS

WHAT IS HAPPENING IN THE WORLD

Definition of Cyber Crime

Cybercrime, or **computer-oriented crime**, is a crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target.[2] Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or mental harm, or loss, to the victim directly or indirectly.

- US Department of Defence

WHAT IS HAPPENING IN THE WORLD TODAY?

WHAT IS HAPPENING IN THE WORLD

December 2012 | Moroccans hack SA government. The Department of Social Development, the Presidential Planning Commission and the National Population Unit's sites were all hacked by "H4ksniper", which linked to a Facebook account of someone called Moroccan Haksnipx. Luckily no sensitive information was reportedly accessed or release.

Jan 2012 | Postbank lost R 30 million in a high tech heist by cybercrime syndicate with in-depth knowledge of the Postbank IT systems.

June 2016 | Standard Bank South Africa w
syndicate - the bank lost R300m through A

Home / Newsroom / King IV Report – The Importance of Corporate Governance

King IV Report – The Importance of Corporate Governance

This article is more than **7 mo**

$32m stolen fr
exchange in lat

SA's average d
R43.3m

By Admire Moyo, ITWeb's news editor.
Johannesburg, 24 Jul 2019

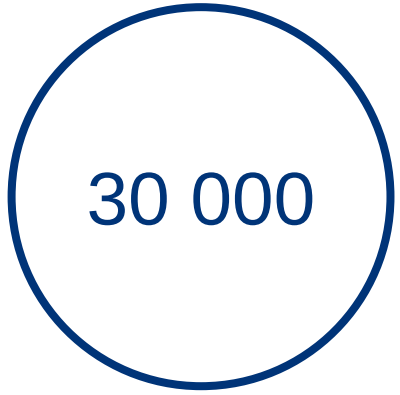
€11.5 million
ions

ıpervisory
ad imposed two
separate fines of €8.5 million and €3 million on Eni Gas e Luce (EGL), an...

INTERESTING FACTS

Records stolen every second by hackers

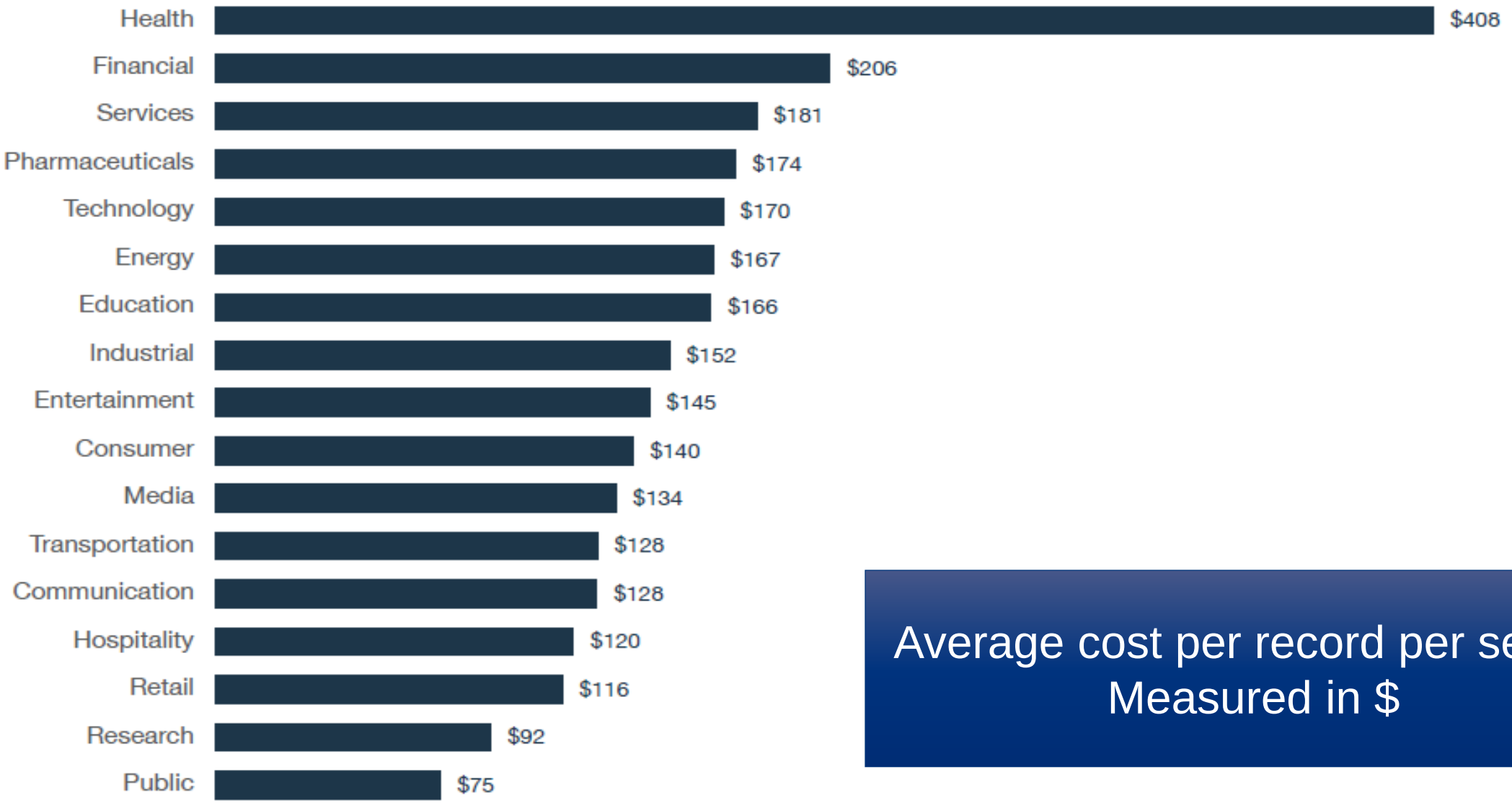
Data breaches are as a result of human error **Phishing or Business process errors**



Websites are hacked daily

Average cost of a stolen record on the black market.

COST PER SECTOR



Average cost per record per sector. Measured in $

Source: Cost of a Data breach: Ponemone Institute 2019.

COVID19 IN CONTEXT OF CYBERCRIME ?

COVID19 IN CONTEXT

- 21 day lock down to prevent the spread of the Corona virus.
- This has resulted in unprecedented amounts of “work from home” situations.
- Very few organisations have catered or prepared for this type of scenario in their Business Continuity Planning (BCP) - most have Disaster recovery sites, but not work from home for the entire business.
- All types of employers and employees are vulnerable – Why?
  - People are more relaxed at home then work. The mindset of “Cyber crime only happens in the office”
  - Remote working users do no always have Anti-virus software and/or Virtual Private Network (VPN) software
  - Home computers are rarely protected with Anti-virus or personal firewall software.

Perfect play ground for a Cyber Crime/Hacker

TARGETED INDUSTRIES

WHO ARE THE TARGETS AND WHY?

- **Everyone remains a target – Cyber criminals have no discrimination – they start from the weakest link.**

All Home working users

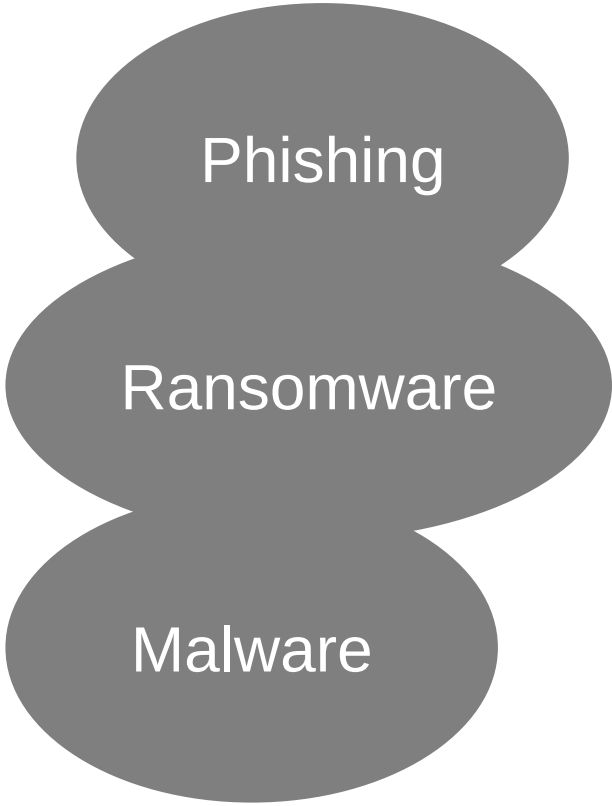
- **Little to no anti-virus software.**
- **No personal firewalls.**
- **Not all work computers have secure linking software such as VPN.**
- **Spending a lot more time on line**

SME's

- **Do not often have the budget to spend on security software, monitoring tools and resources.**
- **Move to offer on-line services/purchases – with little consideration for IT Security.**

Health/Medical Industry

- **Hackers are already claiming to have sequence pathogen formulas – in return for Crypto Currencies.**
- **In the USA and UK, scams has already been reported of sites offering Ventilators, Masks, etc – you pay, but no delivery.**



PHISHING AND FORENSICS – CASE STUDY 1: PROJECT GHOST

Background

- Criminals target certain hotspots like casinos and approach individuals that work with certain Departments, for example, Health
- The individuals targeted often have some type of uniform or other identification to ascertain their place of employment
- They offer the employee some type of gratuity for doing them a favour
- The favour involves inserting some type of device into the computer systems of the employer or providing a free device such a memory stick, etc.
- Unknown to the employee the device contains some type of malware which is introduced to the employers computer systems

PHISHING AND FORENSICS – CASE STUDY 1: PROJECT GHOST

Consequences and how discovered

- In this case the finance system was compromised where the criminals obtained key information such as user names and password to access the finance system
- One day, when one of the employees in the Finance Department was on a lunch break, they had seen their mouse moving and certain transaction were performed. They thought it was ***Ghost*** moving their mouse
- The end result was that criminals were actually transacting on the employee's profile and misappropriating large amounts of money into their own bank account

- Today there are more sophisticated methods of deploying different types Malicious Software or Trojans
- These include: webcams, key loggers and spoofed websites, etc. to obtain confidential information

PHISHING AND FORENSICS – CASE STUDY 2: PROJECT COVID 19

Background

- Company A (Covid19) entered into an agreement with Company B (Kiel) to supply PC Tablets
- This was the first time that Company A used this supplier and the transaction was initiated by a previous employee
- Malicious Software compromised the email correspondence between the parties, which was fraudulently used to mislead Company A into making a payment into a Spanish Bank Account
- Company B denied that it had issued any instructions to change their payment details from HSBC to a Spanish Bank Account

PHISHING AND FORENSICS – CASE STUDY 2: PROJECT COVID 19

What happened

	Legitimate email address	Spoofed email address
Company A	Covid19.co.za	Covid19-za.co
Company B	Kiel.com.cn	Kiel-cn.com

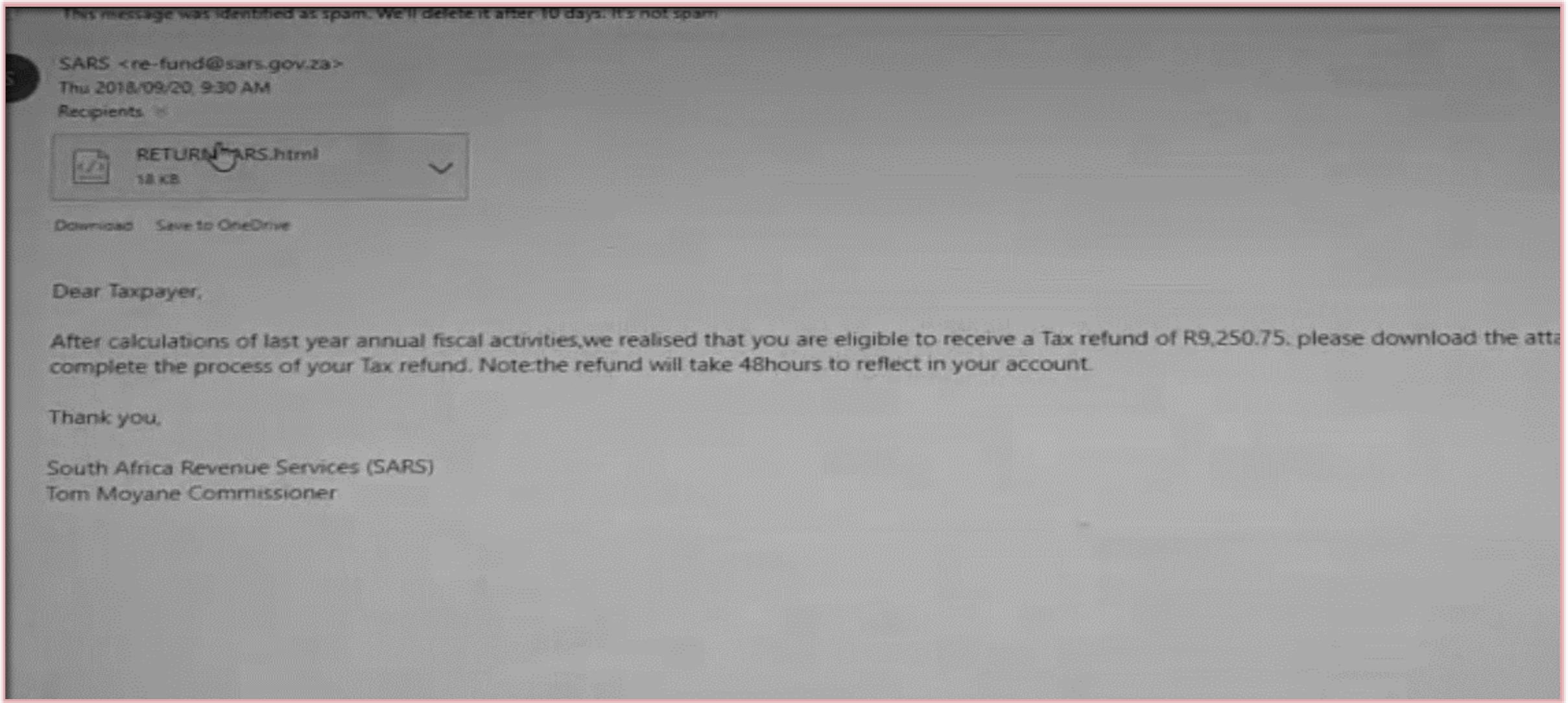
- Criminals sent messages via webmail from where spoofed messages can be sent
  - *hostedemail.com*

- Computer forensic experts found Malicious software on the laptop of one of the employees
  - With the ability to intercept usernames and passwords
  - Infected at the time with "information stealing" malware classified as **"*Trojanzbot*"** and **"*darkcomet*"**
  - It was introduced to the laptop via an attachment ***"swift.rar"*** via an email address

- **Recommendation**: scan devices with at least 3 anti-virus software

PHISHING AND FORENSICS – CASE STUDY 3: FAKE WEBSITES

What happened



PHISHING AND FORENSICS – CASE STUDY 3: FAKE WEBSITES

What happened

WHAT CAN I DO TO SAFE GUARD MY ORGANISATION AND MYSELF?

REMOTE WORKING CHECKLIST

In light of the recent announcements from our Government regarding COVID-19, we have realized that most, if not all employers are allowing employees to work from home and/or remotely in a quarantined area.

Mazars has provided a checklist and a list of dos and don'ts for employers and employees respectively.

EMPLOYERS/CISO/CRO/CIO

WHAT TO DO:	CHECK
• Ensure laptops have up to date Anti-virus software and that scanning of USB ports are enabled.	○
• Ensure the relevant Virtual Private Network (VPN) software is enabled and/or two factor authentication (2FA) is implemented.	○
• Where possible, ensure hard disk encryption with maximum password requirements are applicable.	○
• Ensure that the remote work security policies are the same as working on the network in the office.	○
• Deploy collaboration software on laptops ahead of time and avoid staff downloading and/or configuring software independently or via written instructions.	○
• Remind staff to change passwords as per the password policy, but do not extend the period of password changes e.g. 30 days to 90 days.	○

EMPLOYEES

- ✓ Ensure you are able to login to the network with a password.
- ✓ Do not plug foreign or unapproved Memory sticks into laptops.
- ✓ Only visit web sites that are work related or deemed safe. Check with your IT Department if unsure.
- ✓ Report any strange emails or activities you notice with your laptop or pc.
- ✓ Load anti-virus software and personal firewalls on your private/personal computers.
- ✗ Visit websites that are deemed unsafe or unfamiliar.
- ✗ Do any banking or transactions if the website does not have HTTPS: in the start of the URL.
- ✗ Provide any confidential information to anyone requesting it unless you have prior knowledge of the request.
- ✗ Respond to any emails that is COVID-19 related requesting information.
- ✗ Respond to any emails or requests for personal information or company related information.

QUESTIONS

CONTACT

Terence Govender

Director – IT Advisory

Terence.Govender@Mazars.co.za

021 818 5000

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in 91 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in the Mazars integrated partnership and 16,000 via the Mazars North America Alliance - to assist clients of all sizes at every stage in their development.

*Where permitted under applicable country laws

MAZARS