

# Abuse of personal information Managing on-line fraud & data breach risks

FISA Conference  
Steven Powell  
17 October 2023



# Agenda - Managing Cybercrime Threats

- Introduction
- Attacks on individuals
- Identity theft
- Change of bank account fraud
- Risk Mitigation measures
- Cybercrime risk assessments
- Cybercrime response plans
- Social media sharing risks
- EFT fraud
- Questions



# The Covid 19 Pandemic has been a nightmare that none of us ever dreamt we would experience

- **There has been a further epidemic** - During Covid 19 - Cybercrime is said to have become the second largest threat with a near 300% global growth
- Hackers have taken advantage of the “new normal” uncertainties and remote working to spread malware embedded in malicious links; phishing smishing and pharming emails have proliferated to unprecedented levels
- Man in the middle attacks – cloning of invoices – everyone is at risk!
- Ransomware attacks have reached staggering proportions, emphasizing need for remote backups
- Crypto frauds are rampant - Extensive legislative provision been made globally in respect of virtual assets and VASPS – many cases exposed
- Organizations have had to invest in strengthening and improving ICT resources and cybersecurity strategies to ensure business continuity
- Training on Cybersecurity is critically important to ensure that employees recognize potential threats and avoid clicking on malicious links



# The cybercrime threat

- SA under siege: *Gov calls for global help to combat cybercrime – “South Africa loses approximately R2.2 billion per year to cybercrime. Parliament has called for global cooperation”*

*The Citizen 15 March 2023*

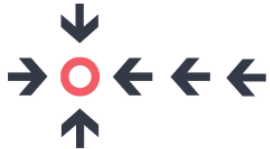
- South Africa has the third highest number of cyber crime victims worldwide,
- Every time you log onto your smartphone, computer or open an email, you are at risk of being exposed to cyber crime.
- The cyber threat landscape is vast and no one is immune.
- And it’s not just big businesses who are vulnerable to the growing incidence of cyber attacks.
- Individuals are regularly targeted with crimes.



# Cyberattacks are not stopping any time soon, and in fact, are getting more sophisticated.

## 59%

of respondents say cyberattacks are growing increasingly sophisticated



## 75%

of companies have experienced an increase in email-based threats



## 72%

of companies expect to be harmed in 2023 by a collaboration-tool-based attack.



For cybercriminals, however, email remains the primary route of attack; in fact, the State of Email Security (SOES) study found corporate reliance on email continues to grow at a rate outstripping the surge in email that took place at the outset of the COVID-19 pandemic — with 82% of companies reporting a higher volume of email in 2022, compared with 79% in 2021 and 81% in 2020.

**But while the increasing number of threats is a problem, their growing sophistication poses an even greater danger.**



# Global impact of cybersecurity breaches

2023

**33 billion**  
electronic records are expected to be **stolen** <sup>4</sup>

**\$8 trillion**  
Cybercrime is expected to **cost the world** \$8 trillion. In economic terms, this is greater than the GDP of any country except the U.S. and China<sup>5</sup>

**\$4.35 million**  
Globally, the **average cost** of a data breach is \$4.35 million. The average cost in the U.S. is more than double that, at \$9.44 million<sup>6</sup>

**13%**  
There was a 13% rise in **ransomware** in 2022 — an increase as big as the past five years combined<sup>7</sup>

**212 days**  
On average, it takes 212 days to **detect** a data breach and another 75 days to contain it<sup>8</sup>

**The cyber threats that have captured management's attention are daunting.**

Mimecast – state of email security report 2023

## The terrible Trio Phishing, Ransomware & Spoofing

- There were an estimated 255 million phishing attempts in 2022, a 61% jump over the prior year.
- Worse yet, more than 70% of these emails were opened by the recipient.
- Two-thirds of this year’s SOES respondents (66%) reported falling victim to ransomware, but in this case, it was smaller businesses that were affected more severely.
- Email spoofing remains a serious risk, especially for the public sector.
- Nearly all SOES respondents (91%) were aware of attempts to misappropriate their email domain, and close to half (44%) saw increases in this type of activity in 2022.



# Cyber Crime - attacks on individuals

- ✔ **Social Engineering** - used by criminals to gain personal or confidential information from an unsuspecting victim.
- ✔ **Identity theft** - where criminals obtain information about you to convince a bank or a customer service representative that they're you. Also described as **spoofing** - the criminal impersonates another individual or organization, with the intent to gather personal or business information so that they can transact in your name. (incur credit, redeem investments, claim tax refunds etc.).
- ✔ **Phishing** - where criminals attempt to trick unsuspecting individuals into clicking on a malicious URL or e-mail attachment to steal their login details which they can then use to gain unauthorized access to the victims' financial accounts.
- ✔ **Vishing** - when a fraudster phones a victim posing as a bank official or service provider and uses social engineering skills to manipulate them into disclosing confidential information.
- ✔ **Smishing** - short for SMS Phishing, is where criminals send an SMS often purporting to be from your bank requesting your personal or financial information such as your account or PIN number.



# Cyber Crime - attacks on individuals... continued

- ✦ **Pharming** - this is a cyber attack intended to redirect a website's traffic to another, fake site - a malicious website that resembles the legitimate website, used to gather usernames and passwords.
- ✦ **Ransomware** - this is where a hacker encrypts files on your computer. The only way to get the files back is to pay the hijacker in crypto currency, like Bitcoin.
- ✦ **Advance Fee Frauds** - you need to pay an upfront fee to claim your “prize”. (OMO, Lottery, SARS, puppy scams, etc.)
- ✦ **Man in the Middle attack** - this is also known as business email compromise where a hacker gains access to your mailbox and send out mails impersonating you. (redeems investments, changes your bank account, etc.
- ✦ **Romance scams** - after a few emails you are suddenly are the love of their life and they will soon need money from you to overcome a crisis.
- ✦ **419 Scams** - this is the famous Nigerian letter purporting to be from a foreign diplomat who needs to use your bank account for a payment.





# Theft of personal data - **identity theft**

The unlawful use of someone else's personal information

For example

- ID / Passport / Driver's licence
- death certificate
- marriage certificate
- letters of executorship
- salary advice
- municipal bill
- bank statements
- Login details - username / password

## Organised Crime



# Data sources exploited in identity theft?

- Hacking of mail accounts BEC – man in the middle attacks
- CIPC
- DEEDS
- Natis
- Credit checks

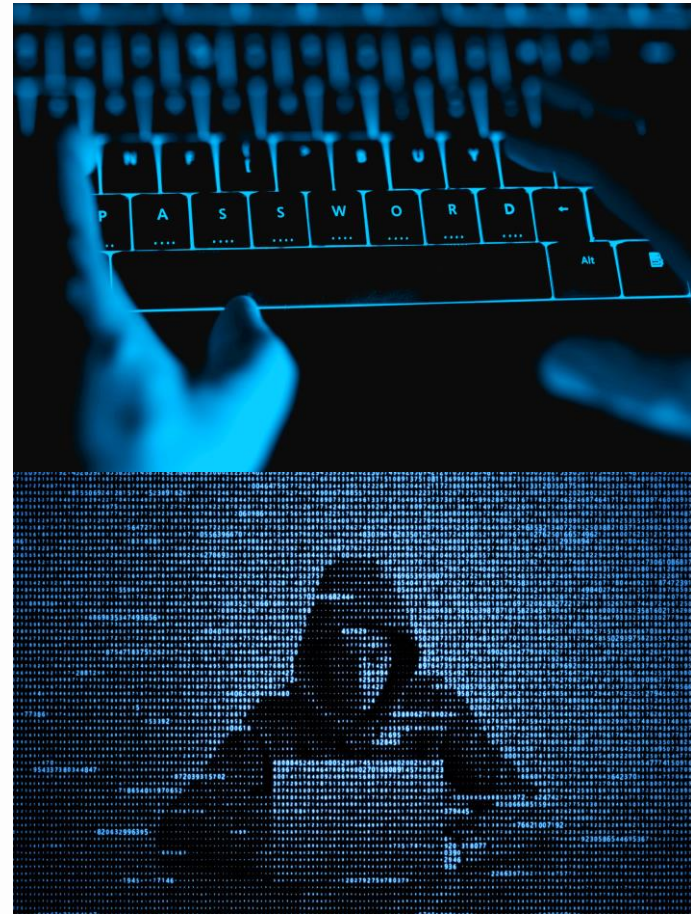
Case study example



# What syndicates do with this info

Fraudulent ID factories create authentic looking docs to

- Open new retail or credit card accounts
- Submit false claims/redemptions re
  - investments
  - insurance
  - medical aid
- Impersonate you transact in your name
- Open companies in your name on CIPC
- Change bank accounts
- Receive tax refunds/redemptions payments



# Change of bank account fraud/BEC attacks/man in the middle fraud

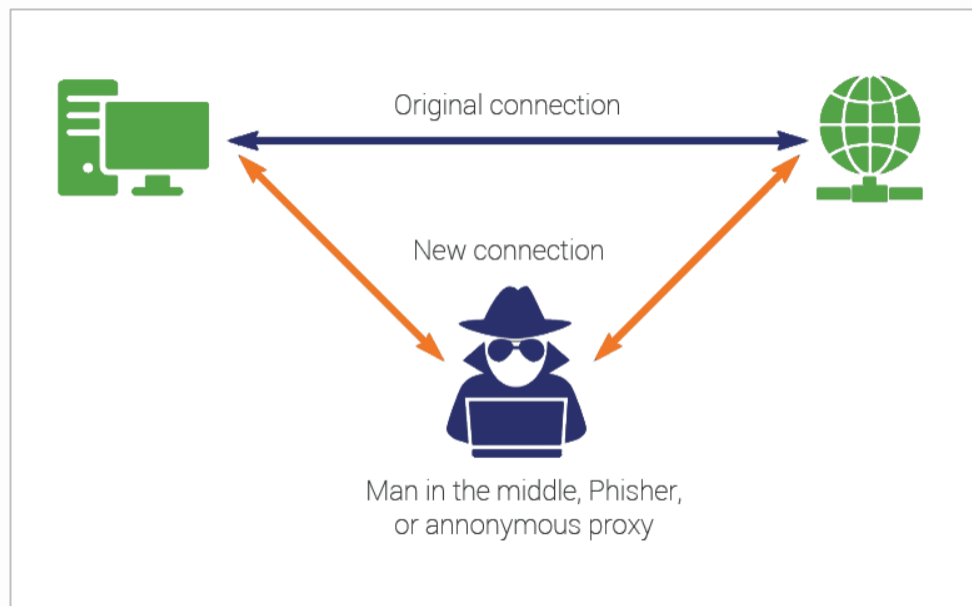
- This is a form of corporate identity theft
- Invoices intercepted in the mail
- Details are cloned
  - NEW BANK ACCOUNT DETAILS are inserted
  - Everything else looks identical and legitimate
- What are the clues to cloned invoices?

1. Changed bank account
2. Cell no.
3. E-mail - gmail



Who is liable for fraud caused by BEC?


## Man in the middle or business email compromise (“BEC”)



The attacker **secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.** Fraudsters use hacked email accounts to convince businesses or individuals to make payments that are either bogus or similar to actual payments owed to legitimate companies.



# Phishing & pharming

 Tue 2016/10/25 10:23 AM  
Online <leon@ibc-bsa.co.za>  
Uncleared R17,225 made to your acc 91001


To: Werner Jordaan

**ABSA**  
Dear valued customer

As received, new MPL paid to your acct was unsuccessful. Kindly continue to finalise.

Proceed now [for more info.](#)

Thank you.

 Tue 2016/10/25 10:23 AM  
Online <leon@ibc-bsa.co.za>  
Uncleared R17,225 made to your acc 91001

To: Werner Jordaan


**ABSA**  
Dear valued customer

As received, new MPL paid to your acct was unsuccessful. Kindly continue to finalise.

Proceed now [for more info.](#)

Thank you.

[http://www.livinstonecollegegroup.com/demo/css/help.php?\\_tsak=344&mxk=3cybmvyqgn5yw5yzs5jby56yq==ce4d2v28&irgk=12](http://www.livinstonecollegegroup.com/demo/css/help.php?_tsak=344&mxk=3cybmvyqgn5yw5yzs5jby56yq==ce4d2v28&irgk=12)  
Click to follow link

 Wed 2016/11/16 10:58 AM  
Revenue Service <dmroux@waikato.ac.nz>  
Get your refund NOW

To: Werner Jordaan

**SARS eFILING**  
New refund due to you.. Kindly continue below to accept payment immediately.

You have received this message on the basis of the following tax type:

- Corporate Income Tax
- Customs Duties
- Pay As You Earn (PAYE)
- Personal Income Tax
- Provisional Tax
- Unemployment Insurance Fund
- Value Added Tax (VAT)

For processing, [please continue here.](#)

[Click to follow link](#)

[VISIT NOW >>](#)

Sincerely,  
SARS Team

<http://www.erinniehenke.com/wp-includes/text/diff/css/coach.php?mxk=ycybmvyqgn5yw5yzs5jby56yq=ku bd2v28&metaid=8f&controlpad=e7f>  
Click to follow link



# A recent attack

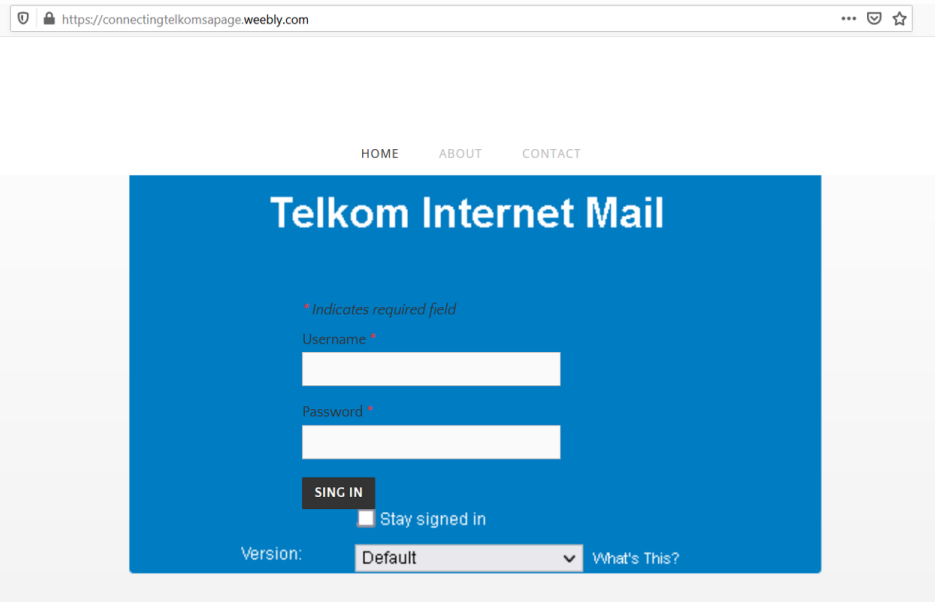
Hi , xxxxxxxxxx

We would like to come to your notice that the previous FNB primary account submitted to you is undergoing internal auditing. So it's not linked to the new one, we are temporarily unable to use it . The new Fnb account is our subsidiary account and let this serve as an authorisation to effect the payment into the account.

We sincerely apologize for the inconveniences caused.

A quick response and advice of payment from you would be much appreciated.

XXXXXX





# The FNB account confirmation

HI THERE, MORNING

KINDLY FIND BANK CONFIRMATION LETTER BELOW FOR OUR UPDATED BANK ACCOUNT. PLEASE MAKE USE OF THE NEW ACCOUNT FOR PAYMENT AND FORWARD REMITTANCE ONCE = =3D PAYMENT IS DONE. CAN WE EXPECT PAYMENT TO BE DONE TODAY ?

XXXX

Date: 2023-06-26

To whom it may concern

### ACCOUNT CONFIRMATION LETTER

We confirm that **\*CHANS AUTO (PTY) LTD** with identification/registration number **2020765112/07** ("the account holder") holds the following account with First National Bank, a division of FirstRand Bank Limited ("FNB"):

Account Type	GOLD BUSINESS ACCOUNT	Account Number	63001119329
Account Status	Active Account - The account is currently open and transacting		
Branch Code	250 655	Branch Name	NEW PARK
Swift Code	FIRNZAJJ	Date Opened	2020-10-13

FNB issues this letter at the specific request of the account holder and for informational purposes only. This letter serves only to confirm that the above information is, according to the records available to FNB, factually correct as at the date of this letter.

Accordingly, FNB provides no warranties, guarantees, assurances or undertakings of any nature in connection with the above information, the account and/or the account holder, cannot be held responsible for any reliance which may be placed on this letter.

Without limiting the above in any way:

- (i) This letter does not constitute a letter of guarantee or a letter of credit.
- (ii) This letter does not imply or infer in any way that FNB has reserved the funds held in the account in favour of any person, nor that FNB has placed a hold on or limited the amount available in the account. The amount available in the account may change at any time without prior notice to you; and
- (iii) FNB will not be held responsible for any change in the information contained in this letter.

This letter is issued to you without any liability for FNB or its employees. You are to treat this letter as confidential.

Should you have any queries, please visit our website [www.fnb.co.za](http://www.fnb.co.za) or feel free to contact us on 087 736 2247.





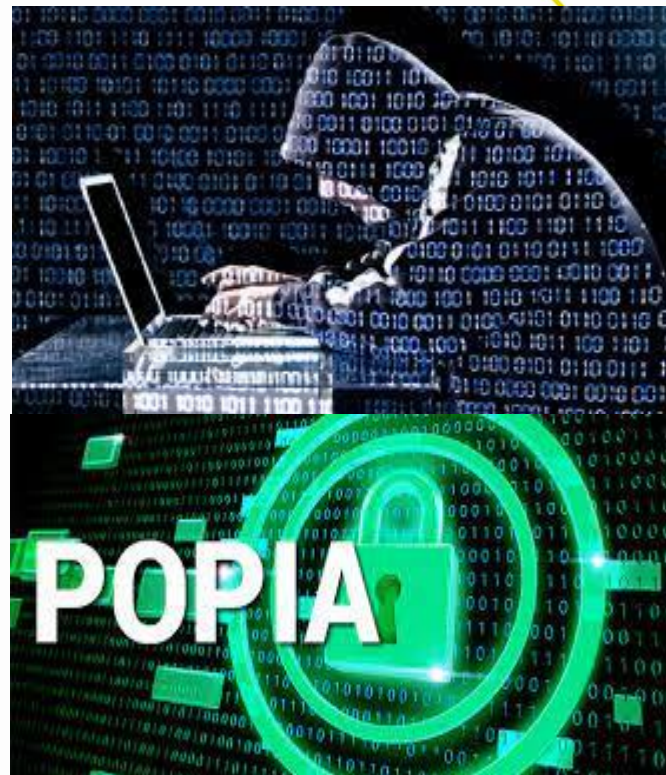
# Consequences of Cybercrime Attacks & Data breaches

- financial penalties
- criminal liability and imprisonment
- business interruption / loss of profits
- asset damage
- ransom
- reputational damage
- third party damages' claims
- legal costs



## the nightmare situation of a Cybercrime attack – a data breach!

- Section 22 of POPIA – breach notification:
  - “Where there are reasonable grounds to believe that the **personal information** of a data subject has been **accessed or acquired** by any **unauthorised person**, the responsible party **must notify**...”
    - (our emphasis)
- **who?**
  - mandatory notification to the Regulator in all circumstances
- **when?**
  - “as soon as reasonably possible”
- **how?**
  - to the Regulator
  - to the data subject



# defending and mitigating data breaches

The Information regulator will want to know how you responded and how you have mitigated the risk of recurrence

- incident response plan / security compromise plan
- incident response team
- legal advice – legal privilege and proper reporting (Regulator & Victims)
- tailored cyber insurance policy and appropriate insurance cover

These are all useful BUT few companies invest proactively in mitigating cyber risks - Prevention is better (and cheaper) than cure

- The Cybercrime risk exposure
- Cybercrime policies and procedures
- Training on Cybercrime risks – Building the HUMAN FIREWALL



# How to minimise the risk

There are people who gather personal information about you in order to access your funds. Therefore make sure that it is difficult for strangers to access your personal information

## What must I do?

- Shred sensitive documents
- Make sure all your accounts have strong passwords that are not easy to decipher
- Never respond to an e-mail or sms that asks you to insert or update your personal and banking information by clicking on a website link



## How to minimise the risk... cont'd

- Be very selective with the type of information that you share on social media - case study
- Use strong passwords, -variety of upper case and lower-case letters, symbols, & numbers. Never write them down where other people can see them. You should also try change them frequently.
- Only use reputable online shopping sites. Use secure sites and check with friends if they've heard of it or used it before.
- Be extra cautious when using Wi-Fi hotspots. Scammers falsify popular hotspots.
- Don't click on random links.



# conclusion

- Corporate and individual ID theft and digital fraud are significant risks
- Protecting personal data is critical
- Be extremely cautious when transacting on-line and don't overshare personal info
- Perform cybercrime risk assessments
- Have a cybercrime response plan and response team in place
- TRAINING TRAINING AND MORE TRAINING – building a solid human firewall is critical
- Do not work in a vacuum - use the tools, technology & call the experts (EARLY)
- When a breach happens – manage your reporting and mitigation
- Manage this risk proactively – prevention is better than cure!



# questions



Steven Powell  
spowell@ENSAfrica.com  
+27 82 820 1036



Africa's largest law firm

**ENSAfrica.com**