Western Cape Government
BETTER TOGETHER.

ISSUE 19 IMPACT

Don't be a victim of Fraud!

COVID-19 and cybercrime surge

The urge to protect our families and loved ones during the COVID-19 pandemic period is greater than ever before, but what about protecting our organisation and ourselves from the fraud schemes that have now become prevalent, as fraudsters seek out innovative ways to profit from us? We must remain vigilant, both at work and home, to ensure that we don't become a victim of fraud during these troublesome times.

Fraud is the unlawful and intentional making of a misrepresentation that is harmful to another.

A survey done in South Africa by the consumer credit reporting agency, TransUnion, during May and June 2020 revealed that 38% of SA Consumers were the target of cybercrime related to COVID-19 and that 5% of these respondents fell victim to the cybercrime attempts. The top 3 scams are unemployment scams, third party seller scams (on legitimate online retail websites) and phishing.

Data theft is one of the most common types of cybercrime and is the act of stealing information stored on an organisation's computers, servers and other devices. The aim is to compromise privacy by obtaining confidential information from an unsuspecting victim. In our organisation, supplier information such as their banking details, and employee personal information (such as ID number and banking details) could be a target as this data could be valuable to those seeking to use the data for fraudulent means.

The WCG has mechanisms such as multi-factor authentication for accessing resources and firewalls on the perimeter network in place to prevent data theft from occurring. Microsoft Bitlocker, OneDrive for Business and Advance Information Protection are used to encrypt information and to protect the organisation against possible data losses.

LET US LOOK AT A FEW SCAMS THAT ARE OUT THERE:

Advance fee scam

The scammer, who have targeted WCG departments, begins by setting up a website selling unique COVID-19 related products or services. They then send out ficticious RFQ's (Request for Quotation) to suppliers pretending to be from a government department. When the suppliers conduct research on this unique product, they come across the website, where they are required to make payment. Once payment is effected, the fraudster disappears with the money and the supplier never receives the goods

Spoofing at the workplace

Spoofing occurs when someone pretends to be someone else in order to gain a victim's confidence, get access to a system, steal data or spread computer viruses. An individual within an organisation receives an email from an email address that appears to be legitimate, making an urgent request that would require the recipient to reply to that email.

The WCG has been a target of spoofing but thanks to observant and quick thinking officials who received such emails, cybercriminals were prevented from gaining access to the WCG network. These officials noticed that, upon clicking "Reply", the email address changed to a different address, not resembling the email address of the purported sender, and raised alarm with CeI.

The WCG CeI keep ahead of the spam and phishing emails from WCG email addresses. The Messaging and Collaboration team work on providing additional methods of protection for email users such as migration to Azure Cloud Service and Office 365 Advanced Threat Protection. This ensures better messaging hygiene which in turn reduces phishing attempts and spoofing.

Authorised push payment fraud

A hacker gains access to your data and network by you clicking on a phising email link. The hacker is then able to monitor all of the incoming emails that you receive and waits patiently for emails containing invoices for payment of goods and services. The hacker then intercepts this invoice before you access it, and changes the banking details on the invoice to their own banking details.

The person responsible for making payments proceeds to pay the invoice, unaware that the banking details belong to the fraudster and not the legitimate service provider. This scheme is called authorised push payment fraud as the payment is authorised and paid in a legitimate manner, however payment is made into a fraudulent bank account.

(Note: The WCG's processes guard against unauthorised changes to banking details of suppliers)

Scam via smartphone

A smartphone user receives an SMS claiming that he/she has won the lottery and is instructed to click on the hyperlink in the SMS to claim "a" prize. By clicking on the link, the recipient of the SMS is directed to a website containing malicious software created by cyber criminals. Unknowingly, by clicking on the link, malicious software is downloaded, which provides cyber criminals with access to the smartphone, which could contain banking information and particulars of all his saved contacts.

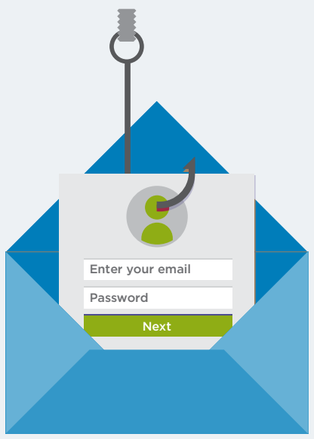
Identity theft

There are many scams aimed at stealing a victim's identity. The 2 scams discussed below have been prevalent in the Western Cape during the pandemic.

- The first one involves fraudsters posing as medical professionals who trick people into handing over their personal information.
- In the second one, criminals capitalised on the Province's widespread unemployment due to the pandemic. Fraudsters pretend to be representatives from HR departments and convince people to submit sensitive financial information as part of the application process for a job that does not exist.

Phishing is when scammers try to obtain sensitive information such as usernames, passwords and personal particulars by disguising their email to be from a trustworthy source.

WHAT DO FRAUDSTERS DO WITH YOUR INFORMATION?



Once fraudsters gain access to your personal information, this information is likely to be sold to other criminals. The sale of stolen records on the black-market averages around R4 000 per record. According to Terence Govender of IT Advisory at Mazars SA, the most valuable records on the black market are health records, financial records and employment records. These records are considered valuable because they can be used in a number of ways for financial gain - criminals make purchases or enter into other financial transactions using the victim's identity and personal particulars or they use an organisation's client list to commit an advance fee scam.

PROTECT YOUR ORGANISATION

- **Login details –** Ensure that you use strong passwords (combination of letters, numbers and special characters) and that you change your passwords regularly.
- **Do not share –** It is important to keep your passwords and login details confidential.
- **Clicking on links –** Now that you know phishing scams exist, be vigilant and don't click on suspicious emails that contain links.
- **Security awareness –** Take note of the various emails sent by CE-I to create awareness around email attacks and working securely while working remotely. Take note of emails relating to POPIA awareness.

PROTECT YOURSELF

- **Personal details –** Don't provide your personal details to callers unless you have verified that the person you are speaking to really represents the organisation they say they're calling from. If in doubt don't answer any questions and end the call.
- **Do not be swayed –** Cyber criminals can be charming, persuasive and convincing. Remember that if it sounds too good to be true, then it most likely isn't true.
- **Everyone is fair game –** Criminals do not distinguish between the educated/uneducated, employed/unemployed, old/young, poor/rich. Don't believe that they will never target you. Remain cautious, alert and wary – it is your best protection.

Provincial Forensic Services are mandated to investigate matters relating to fraud, theft and corruption in the WCG. You can report these matters via:

Telephone on 021 483 0931 | Email to: tip.offs@westerncape.gov.za
National Anti-Corruption Hotline on 0800 701 701