PSA The Union Of Choice

INFORMUS

SINCE 1920 still driven by SERVICE EXCELLENCE

FOR PSA MEMBERS: **GENERAL 6/2023**

09-03-2023

Ransomware attack Public Service Bargaining Councils

The Public Service Coordinating Bargaining Council, General Public Service Sectoral Bargaining Council, and the Safety and Security Sectoral Bargaining Council experienced a cyber-attack on their information communication technology system (ICTS) from 24 to 28 February 2023. This created major challenges for these Councils to perform their core functions as the entire ICTS has been compromised. These Councils are currently unable to fulfil their statutory and contractual obligations in respect of dispute management.

A *force majeure* was invoked on dispute resolution processes from 1 to 31 March 2023. During this period, the Councils will focus on processes to recover information and restore operations whereafter a further assessment will be done to establish readiness to proceed with obligations.

It is therefore important to inform members that they will not be able to refer new disputes to Councils or have current disputes schedules for this period. Case of file reconstructions and filing matters at court will be affected. Referrals or other disputes process linked to time frames will be condoned for the period of the *force majeure*.

Members are urged to be alert as hackers are taking control of networks, locking away files, and demanding ransoms to return data to the rightful owners.

How to protect yourself

Members are urged to be careful and avoid falling victim to cybercrime. Follow these helpful tips to protect yourself:

DO NOT:

- Disclose any card security details such as your PIN number, internet banking log-in details or card number over the phone, by email or text message or via a link included in an email or text.
- Feel rushed or pressured into making a decision. No genuine bank or other legitimate organisation would ask you to carry out a transaction on the spot.
- Assume that an email, phone call or text message is authentic. If in doubt, hang up the phone or delete the email or text message without opening it.
- Click on links or attachments included in unsolicited emails or text messages.

DO:

- Call companies back using the number on their website. If you are unsure whether a phone call, email or text message request is genuine, it always best to call the organisation back using the number on its website to confirm.
- Check email addresses, phone numbers and URLs carefully – do they look suspicious?
- Install up-to-date anti-virus software on your devices.
- Follow the ABC framework for fraud: Accept nothing, Believe no-one, and Confirm everything.
- Slow down, think before you click. Anything that is too good to be true should be treated as suspicious.

What is…

Phishing: A cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Smishing: Follows largely the same pattern as phishing but takes place over text (SMS) or messaging services such as *WhatsApp*.

Vishing: Unlike phishing or smishing, vishing refers to over-the-phone fraud where criminals will call you, posing as your bank or another seemingly reputable company, to verbally obtain sensitive data such as passwords, addresses, *etc*.

Ransomware: A form of malicious software (also known as malware) designed to encrypt data on a user's device, making it inaccessible to them until they pay a ransom to the attacker. Ransomware can be downloaded in many ways, such as clicking on suspicious links and installing illegitimate files.

The PSA will however closely monitor this situation and keep members updated.

GENERAL MANAGER