OPINION PIECE

GIPF
Government Institutions Pension Fund
To guard, and to grow.

FOR IMMEDIATE RELEASE

11 JANUARY 2022

Cyber Security Protection tips for the new year.

The Government Institutions Pension Fund (GIPF) has in recent years increased the shift and reliance in the use of information technology for its staff and members. As we aim to reduce the further spread of the COVID-19, we encourage our members to make use of our online platforms such as the GIPF member portal, our regional call centre lines and regional emails addresses, to access our services. The Fund pleads with members to always remain vigilant when using our online platforms specifically, the member portal. We encourage members to keep their passwords private.

It's the dawn of a New Year and as such we reflect on a very difficult year when it comes to Covid-19. During this time, everyone is in a joyous, celebratory and free-spirited mood yet others are quite anxious about the year ahead. With an entire year upon us, certain individuals dread thinking about what the year holds for them due to financial constraints. It is with this background in mind that I wish to caution our members to be observant when it comes to their finances.

Mischievous people will approach you for their own benefit to rob you of your hard-earned savings. They are prone to use the following vectors;
Personal and Electronic Scams such as:

1. Emails
2. WhatsApp
3. Text messages and,
4. Phone calls.

Before responding to prompts via any of the above means of communication, verify the legitimacy of the person contacting you. Where you are requested to share personal information, scrutinize the information again. Refrain from sharing any of your personal information like: Pins, Debit Card/Credit Card Numbers, and any other personal information. When making use of ATMs, swiping your card at any place or making use of online banking, be aware of your surroundings and ensure your personal details are protected.

Below are a few tips to set up complex and lengthy passwords which consists of at least 12 characters when using the GIPF online portal, online banking and email addresses.
When creating your password consider the following:

- Do not use personal information

- Do not make your password easy to guess
- Do not write your password down
- Do not share your password
- Do not use alphabet sequence (abcdef…), number sequence (1234567) or keyboard sequence (asdfghjkl)
- Use a passphrase
- Make it something you can visualize
- Use a mixture of upper/lower case, numbers and special characters

Additionally, we would like to encourage our members and the public to be weary of the following:

1. Increased Phishing and Ransomware Attacks:

Communication via emails has increased drastically during the pandemic and will continue to rise in the near future. Therefore, some people (hackers) with malicious intent also make use of this opportunity to send out emails or direct messages to different social media platforms. These dishonest emails or direct messages often require you to install an executable file that encrypts your data or prompt you to click on a link which will further request you to provide more information about yourself. When you come across such emails, you are encouraged to scrutinize who the sender is as well as the content and it should be familiar to you before you can reply or act upon the mail. However, you may delete.

2. Free Public WiFi/Internet

Restaurants, malls, airports and other public places often provide “Free WiFi” to customers and users. These Free WiFi offerings are often not secured and come with the risk of being breached as hackers know and sometimes see many people making use of their mobile devices. A few risks associated with using public hotspots are: Malware distribution, access to private information and unencrypted networks. I advise you to try as much as possible not to use free Public WiFi offerings as the security around it is not adequate to protect your device compared to what an organisation would put in place.

With the aforementioned, I wish you all a successful, and cyber-crime free 2022!

Written by: Martin Hamukwaya
Information Systems Security Officer - GIPF

#END#