Protect your personal information on social media- warns CSIR cybersecurity experts

South Africans are sharing too much of their personal information on social media, allowing cybercriminals to exploit them for their personal gain.

Cybersecurity experts from the Council for Scientific and Industrial Research (CSIR) have urged the public to be mindful of what they post on social media and to carefully check the permission lists when they download applications (apps).

CSIR researchers, Dr Vukosi Marivate, Muyowa Mutemwa, Nyalleng Moorosi and Thulani Mashiane showcased their research in social mining data, network vulnerability, data science for public safety and cybersecurity awareness at a media briefing in Pretoria this morning, 11 June 2018.

Allowing apps more access on your phone than required could lead to security risks and expose your personal information. Other apps require access to your exact location, revealing details such as your house number, workplace and email account details. Other people still post pictures of their vehicles with a number plate clearly visible for the world to see making it easier for criminals to clone the registration number.

“Be vigilant when you share information on social media”, said CSIR cybersecurity researcher, Thulani Mashiane.

Mashiane said South Africans should stay away from installing suspicious applications and should only download applications from original/reputable website [if !supportAnnotations][TT1] [TT1]or applications store.

“Don’t over share, think before you click. Personal information can be used to answer security questions for certain accounts, identity theft, direct marketing and by stalkers”, she said.

Cybercriminals are also targeting the kids through games, said Mashiane urging parents to check every game the kids are playing.

Mashiane cited one of the game called “Blue Whale”. The game targets mainly vulnerable teenagers by assigning them to do tasks set out, with the final challenge asking the player to commit suicide.

“Parents please check what kids are doing on their phones. Many teenagers are killing themselves because of these games. In this game, participants are expected to share photos of the challenges completed by them. This include cutting themselves, killing animals and eventually killing themselves.”

Speaking on network vulnerability, researcher, Muyowa Mutemwa warned South Africans on using public and open networks for banking transactions.

“Cybercriminals love public open networks such as internet café networks, coffee shop Wi-Fi and conference Wi-Fi. Use secure network for banking, no banking or social networking on public Wi-Fi,” he said.

South Africans are also looking into crypto-currencies investments that promise high returns. It is important to note quick returns are not a solution because we have seen millions of dollars lost when these schemes collapses.

Senior data scientist, Dr Vukosi Marivate conducted a study on social media mining safety and he lead a Data Science team at the CSIR. The team develops social media analytics, mapping and geo-location tools. Applications vary from public safety and crime incident detection on social media, building models for better resource allocation and situational awareness.

Dr Marivate said social media can be used to combat crime. “We are developing a tool to help law enforcement agencies, government and NGO’s in understanding the

trends in crime and public safety."

There are still limitations using social media data, Dr Marivate notes "We need to understand the limits and biases that can be introduced by relying only on social media data that might represent only a subset of the population or perpetuate discrimination given past data."