MINISTRY
COMMUNICATIONS AND DIGITAL TECHNOLOGIES
REPUBLIC OF SOUTH AFRICA

Private Bag X860, PRETORIA, 0001 – iParioli Office Park, 1166 Park, Hatfield, PRETORIA

Tel: +27 12 427 8000 – Email: Media@DCDT.gov.za URL: www.dcdt.gov.za

KEYNOTE ADDRESS BY DEPUTY MINISTER OF COMMUNICATIONS
AND DIGITAL TECHNOLOGIES, HON. PHILLY MAPULANE
AT THE FPB SAFER INTERNET DAY, CAPE TOWN
06 FEBRUARY 2023

Thank you program director,

The Chairperson of the Film and Publication Board, Ms Zama Mkhosi

Ms Maggie Pillay, FPB Council member,

The CEO of the FPB, Dr Mashilo Boloka

CEOs of NEMISA Trevor Rammitlwa and ZADNA Molehe Wesi

FPB Executive members,

Representatives from INHOPE, UNICEF and other partners

FPB Youth Council,

Miss World South Africa, Dr Claude Mashego

Distinguished guests,

Ladies and gentlemen,

Good morning!!

It gives me a great pleasure to address you today on the occasion of the Safer Internet day. Under the theme "**Connect, Reflect, Protect"** we are gathered here to celebrate this international day where we are seeking to bring awareness to the youth in particular about the use and safety of the internet.

Safer internet Day (SID) is a global initiative to raise awareness of online safety issues, the initiative is celebrated in approximately 140 countries on the second Tuesday of the second month of each year to raise awareness of emerging online social ills such as cyberbullying and the dissemination of Child Sexual Abuse Material (CSAM).

SID 2024 marks the 51st instalment of this initiative that was started in 2005 by Insafe, a European network of Safer Internet Centre's (SICs). Insafe is linked to the International Association of Hotline Operators (INHOPE); and has managed to grow beyond the European borders, South Africa through the FPB being one of the countries belonging to INHOPE.

As a member of INHOPE, the Film and Publication Board (FPB) is hosting SID 2024, here in Woodstock, Cape Town, as part of government's initiative to reach out to communities, in this case our young people, to ensure support to our citizens who require critical information to secure their safety particularly on the online space.

As we gather here today, we are reminded of the rapid pace at which our world is evolving. The digital landscape is no longer a separate entity but an integral part of our daily lives. This integration brings immense opportunities but also significant challenges, particularly in the realms of cybersecurity and digital governance.

According to the 2022 Stats SA census and the recent update as of January 2023, South Africa boasts 43.5 million internet users, which translates into an impressive penetration rate of 78,9% among the population of 62 million. This was an increase of roughly 400,000 individuals compared to the previous year. And from this number South Africa is toping the rankings of internet penetration and freedom in the continent. This gives us the edge towards bridging the digital gap and help in global efforts to connect the 2.7 billion people across the world who remain unconnected. However the advances we've made in internet penetration and use, also exposes us to many internet ills such as human trafficking and child pornography.

DIGITAL FOOTPRINT

The internet has brought into our daily lexicon a new phrase that we often use without expanding too much on it: ***Digital Footprint***. In simple terms, the Digital Footprint is the information about a particular person that exists on the internet as a result of their online activity. It is this personal information that can lead to a harmful use of the internet, and Safer Internet Day is a reminder to keep a watchful eye on what personal information is shared on the internet, and how it is being used.

Program Director,

The proliferation of online content that is now readily available for consumption to our citizens through the internet and social media platforms also places the risk of exposure to harmful content.

The internet is a complex platform that we use to transact with banks and to conduct all manner of commercial activities, as well as to communicate and share with the world information that is sometimes sensitive and of a very personal nature. We also use it to access health information, education, and entertainment.

As they say colloquially, the internet is not sleeping, and neither should we.

INTERNET SAFETY

The growth in internet penetration and use is always accompanied by new and serious threats.

While technological transformation introduces greater variety and convenience into our lives, it also opens more and more avenues for people to be targeted by cyber criminals.

International and domestic cyber criminals increasingly view businesses and private individuals as attractive targets for a range of cybercrime.

This 'digital paradox' means that while governments and organisations can offer more services, more quickly, than ever before, yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.

Because we spend an inordinate amount of time on the internet, the risks of cyber crimes are higher. In the latest Global Digital Report, drawing data from several sources and research groups, it was established that South Africa has the highest screentime worldwide, averaging 10 hours a day. In other words, South Africans are regarded as the biggest internet addicts in the world, spending an average of 9 hours and 38 minutes daily connected on any device. This is far higher than the global average of 6 hours and over 2 hours more than the US.

The CEOs of major social media platforms met few days back to deliberate of issues of internet safety and they were met with intense questioning from lawmakers regarding accusations that their apps pose dangers, sometimes deadly, for children. CEOs of Apps such TikTok, Snapchat, X and Meta products like Facebook and Instagram report that they have put and continue to intensify measures to block and prevent users linked with drug dealing and other criminal activities.

CYBER-ATTACKS

Cybersecurity has never been a higher priority, with recent attacks targeting organisations globally in a series of increasingly sophisticated attacks.

The Cybersecurity threat landscape is exponentially growing in complexity aided by the increasing sophistication of threat actors, with threats characterised by speed and scale of propagation.

Critical infrastructure and critical information infrastructures, which is owned and operated by both government and the private sector, has become a strategic imperative especially in the light of recent attacks and so building cyber resilience throughout the national infrastructure is an imperative.

The borderless and seemingly indiscriminate nature of cyber-attacks mean it is of vital importance that organisations fund and implement measures that protect themselves and clients from financial losses, and the organisation from reputational damage and emerging regulatory imperatives.

Increased internet penetration across our country can give rise to sophisticated attacks on our ICT infrastructure.

USING ARTIFICIAL INTELLIGENCE FOR INTERNET SAFETY

In the domain of artificial intelligence, we stand at an inflection point where AI's capabilities are expanding rapidly.

AI can significantly enhance our security defences, offering automated threat detection, rapid response to incidents, and predictive analytics to pre-empt attacks.

But it also raises concerns about AI being used for malicious purposes, like developing sophisticated malware or automating cyber-attacks.

The challenge lies in staying ahead of the curve – utilizing AI to fortify our defences while also ensuring ethical and responsible use.

We must also address the potential biases in AI systems and ensure that our AI-driven security measures are transparent and accountable.

FPB MUST RE-AWAKEN AND BITE

Programme Director, we must appreciate and welcome the interventions made by government to strengthen online safety and to regulate the space. In March 2022, His Excellency, President Cyril Ramaphosa operationalized the Film and Publication Amendment Act (no. 11 of 2019), which significantly expanded the mandate of the FPB from a traditional classification authority to a fully-fledged content regulator whose future objective is to protect the citizens and children against harmful and prohibited content and activities online, including tackling the increasing unacceptable behaviors such as cyber bullying and hate-speech.

The expanded FPB's mandate now include regulating online harms, and outlawed cyber bullying, revenge porn and hate speech distributed in the main on social media platforms. Safer Internet Day, therefore, is a reminder of the importance of this mandate.

However not many people are aware of this expanded mandate of the FPB and their rights protected under the Film and Publication Amendment Act. And therefore I am calling upon the leadership of

FPB to double your efforts in increasing awareness among South Africans about the actions and behaviors outlawed by this amendment act, including revenge porn and hate speech. The FPB must re-awaken and bite, with the new teeth it has been given.

CONCLUSION

As we delve into this critical theme of Connecting, Reflecting and Protecting, let us remember that internet safety is not just a technical matter but a societal one. It is about protecting our way of life in an increasingly interconnected world. The conversations we have here today will echo beyond these walls, shaping our future and that of the society at large. We encourage everyone to come together and join hands to protect our future.

I thank you.

Issued by the Ministry of Communications and Digital Technologies