Phil Mnisi: Eswatini's Cybersecurity Awareness Month

Speech by Mr Phil Mnisi, Governor of the Central Bank of Eswatini, at the National Cybersecurity Awareness Month "Secure Eswatini, be safe online", Ezulwini, 6 October 2025.

* * *

His Excellency, the Right Honourable Prime Minister,
Honourable Minister for Information, Communication and Technology (ICT),
Other Cabinet Ministers present here today,
Honourable Members of both Houses of Parliament,
Chief Executive, Eswatini Communication Commission,
National Commissioner of Police Service,
Esteemed Stakeholders on National Cybersecurity
Government Officials
Captains of Industry
Members of the media
Distinguished ladies and gentlemen

Introduction

It is an honour to stand before you today as we launch our National Cybersecurity Awareness Month. While the 2025 theme is "Secure Eswatini, Be Safe Online," I intend to cover an important component of this theme entitled "Securing Trust: Building a Cybersecure Banking Ecosystem." This subject is particularly important to banking because trust serves as a backbone and is a foundational element in the financial sector, representing the assurance that funds are secure, transactions are confidential, and systems are resilient. In the absence of trust, transactions and investments may decrease. In the current digital environment, trust is closely linked to cybersecurity.

Over the past decade, digital transformation has changed how people conduct financial transactions, shifting from in-person banking to the use of mobile devices. Various innovations have led to faster payment processes. For instance, the Eswatini Payment Switch, developed and launched by the Central Bank late last year, enables instant low-value payments between participating institutions. These changes have positively impacted financial inclusion and economic activity in Eswatini.

Yet, the same digital technologies that bring efficiency and access have also made banks' prime targets for cybercriminals and cyber-attacks. Our licensed banks have not been spared. Some have experienced cyber breaches. We are also aware of fraudulent schemes, such as "facata" scams, targeting our customers.

Cybercrime within the banking sector results in not only significant financial losses, but also substantial recovery expenses and potential systemic risks that may disrupt payment systems and erode market confidence. Most importantly, loss of trust in digital security threatens the stability of the entire financial system, making cybersecurity as essential as managing liquidity and capital in the banking ecosystem.

Role of the Central Bank

The Central Bank is responsible for maintaining financial stability and ensuring the integrity of the financial system. Cyber resilience is an essential element of this responsibility.

In recent years, we have issued guidelines on cybersecurity and cloud computing to provide minimum standards for financial institutions. We continue to strengthen our supervisory frameworks, ensuring that banks and fintechs adopt risk-based approaches to managing cyber threats.

In line with the requirements of the National Cybersecurity Strategy, we are also envisaging the establishment of a Financial Sector Cyber Security Incident Response Team (CSIRT). A benchmarking visit by CBE to a peer Central Bank with a functioning financial sector Security Operations Centre (SOC) has recently been completed. The lessons learned-both in terms of regulatory frameworks and operational models-will guide us as we move swiftly to operationalize a Financial Sector CSIRT. One major advantage we saw is they have is that their Cybersecurity Act, passed by Parliament, explicitly designated the Central Bank as the Financial Sector CSIRT, hence they had the legitimate power to execute their plans, which are collaborated with their Cyber Security Agency. We foresee and may propose a similar approach, depending more on our cybersecurity laws to achieve the same result as we work in partnership with ESCCOM.

Recognizing that cybersecurity is a shared responsibility, we are also setting up initiatives to drive sector-wide collaboration. These will include the formation of a working group comprising representatives from financial institutions, mechanisms for threat intelligence sharing, and the conduct of joint cyber drills.

Building a Cybersecure Banking Ecosystem

Establishing a cybersecure banking ecosystem requires the involvement of various stakeholders, including banks, fintech companies, regulators, service providers, government agencies, and individual citizens, as it cannot be achieved by the Central Bank alone.

For Our Banks:

Cybersecurity should be a board-level priority for financial institutions. The threat of cyber-attacks is a core business risk; therefore, invest appropriately, empower CISOs, and build a security-focused culture throughout the organization.

Regular drills must be conducted, incident response plans must be maintained, and institutions must actively participate in sector-wide simulations. Innovation, too, must be secure by design-embedding security from the earliest stages of system and product development to ensure that customer trust is never compromised.

For Government and Regulators:

We must work together to harmonize national policy, protect critical national infrastructure, and ensure our legal and legislative frameworks keep pace with rapid technological change.

For Our Citizens:

This is where the National Cybersecurity Awareness Month is most critical. We must educate our employees, our customers, and especially our youth. One way the Central Bank supports awareness is through Section 4 of Legal Notice 62 of 2016, which requires financial institutions to allocate budgets for consumer education.

Cyber hygiene must become second nature. Some simple, disciplined steps can make an enormous difference:

Use strong, unique passwords or, even better, a reliable password manager.

Enable Multi-Factor Authentication (MFA) on all accounts.

Be suspicious of unsolicited emails, texts, or calls asking for personal information-the banks will never ask you for your password.

Always accept that you may be under attack.

Significance of Cybersecurity Awareness Month

This month is not for banks alone. It is for everyone, including government agencies, businesses, schools, communities, and citizens. Cybersecurity is not only about complex systems. It is also about adopting simple daily habits, such as using strong passwords, being vigilant against suspicious emails, regularly updating software, protecting personal data, and reporting incidents promptly.

To our banks and financial institutions, I call upon you to continue investing in cybersecurity, embedding resilience into every aspect of your operations.

To our employees, I urge you to remain vigilant, to report incidents without fear, and to treat cybersecurity as part of your professional duty.

To our customers and the public, "you, too, are guardians of trust." By practising safe digital habits, you safeguard not only your own finances but also the stability of our financial system.

Closing

Cybersecurity is no longer optional. It is essential. It is the foundation of digital trust, financial inclusion, and sustainable growth.

As the Central Bank, we reaffirm our commitment to leading and supporting this effort. But we cannot do it alone. Every institution, every professional, and every citizen must play a part.

Let us work together to secure trust, to build resilience, and to ensure that our financial system remains strong and stable in the face of evolving cyber threats.

Thank you very much.