Bank of Namibia

A GUIDE TO UNDERSTANDING CYBERSECURITY AND VIRTUAL ASSETS IN NAMIBIA

MARCH

2024

MS. BARBARA DREYER

Foreword by the Director: National Payment System and Financial Surveillance

The Bank of Namibia's (the Bank) Strategic Plan (2022-2024) and the National Payment System (NPS) Vision and Strategy (2021-2025) serve as the catalyst for digital transformation, primarily focused on modernising Namibia's financial system to promote financial inclusion and foster greater digital adoption. However, the digital transformation journey introduces weaknesses that can be exploited by cybercriminals, as the relationship between payment systems and cybersecurity is deeply intertwined, given the critical importance of securing financial transactions and protecting sensitive financial data. It is imperative to implement effective cybersecurity controls that are in line with the Bank's regulations and best-leading standards to prevent weaknesses from being exploited.

The prevalence of virtual assets and virtual assets service providers within the Namibian economy compelled the Bank, as the trusted entity that has the mandate to safeguard public funds, to mitigate regulatory concerns and public perception through the enactment of the Virtual Assets Act, 2023 (No.10 of 2023). The Virtual Assets Act requires, virtual asset service providers to adhere to specific security standards and implement measures to safeguard consumer funds against theft, hacking, or mismanagement, which in turn means that cyber criminals have no virtual safe haven to defraud the public.

Overall, cybersecurity is paramount in safeguarding virtual assets and existing digital payment methods against a wide range of threats in an increasingly digital and interconnected world. In light of the above, the Bank as part of its consumer education efforts, deemed it necessary to tackle these critical aspects in its latest publication. In closing, the Bank remains accessible to discuss and engage with the public on issues about cybersecurity, virtual assets and other matters related to the NPS.

CYBERSECURITY IN THE NATIONAL PAYMENTS SYSTEM

MR. JACKY NEKOMBA
Senior Analyst: NPS & Virtual Assets Oversight

What a world we live in where consumers can now make banking transactions from the comforts of their homes using mobile banking payment services such as electronic fund transfers and e-money transactions. Consumers expect a safe, convenient, and seamless banking experience hence, the NPS participants continuously introduce new banking services to foster financial inclusion and enhance consumer convenience. However, with new products comes new cyber vulnerabilities and challenges that cyber criminals attempt to exploit.

The Bank requires NPS participants to appropriately protect consumer information and funds to maintain a safe, effective, and cost-efficient payment landscape. The ever-increasing cyber threat landscape can be curbed by being vigilant, fostering a culture of information security, and implementing adequate cybersecurity controls.

TOP CYBER THREATS IN THE NPS

Phishing attacks: Criminals use phishing texts, calls, or emails to trick unsuspecting individuals into revealing their payment information that may be used for fraudulent activities. The public is advised to be vigilant and not give out confidential information such as banking profile username, passwords and PIN codes.

Card Not Present Fraud: This is when criminals obtain sensitive information associated with a bank card, such as card numbers, expiration dates, and Card Verification Value (CVV) codes, without the need for physical possession of the card. This information is then used to conduct fraudulent transactions online or over the phone, where the card is not physically present.

The Human Element: This refers to insider threats or human errors such as clicking on phising site. To minimise the chances of human error, we need to practice vigilance, segregate duties, and regularly attend cybersecurity related trainings.

WAYS TO PROTECT YOURSELF AGAINST CYBER RISKS

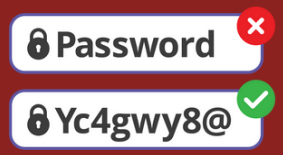
MS. IYISHI GARISES
Senior Analyst: NPS & Virtual Assets Regulation & Licensing

TIPS TO PROTECT YOUR DEVICES

- Update to the latest software.
- Encrypt your data by using reputable algorithm methods and encryption keys to control access.
- Enable strong password to access device.
- Install antivirus software on devices.

KEEP QUIET

Avoid sharing confidential information.

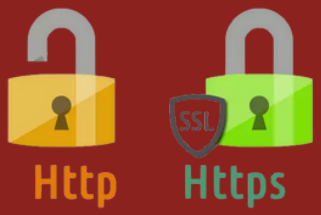


STRONG PASSWORDS TIPS

- The password should be long and hard to guess, with a mix of numbers, letters, and special characters.
- Do not use the same password for everything.
- Change your password for your various things on a regular basis like each month.

MONITOR YOUR ACCOUNTS REGULARLY

- Frequently review payment notifications and bank statements for any anomalies.
- Notify your bank of any suspicious transactions.



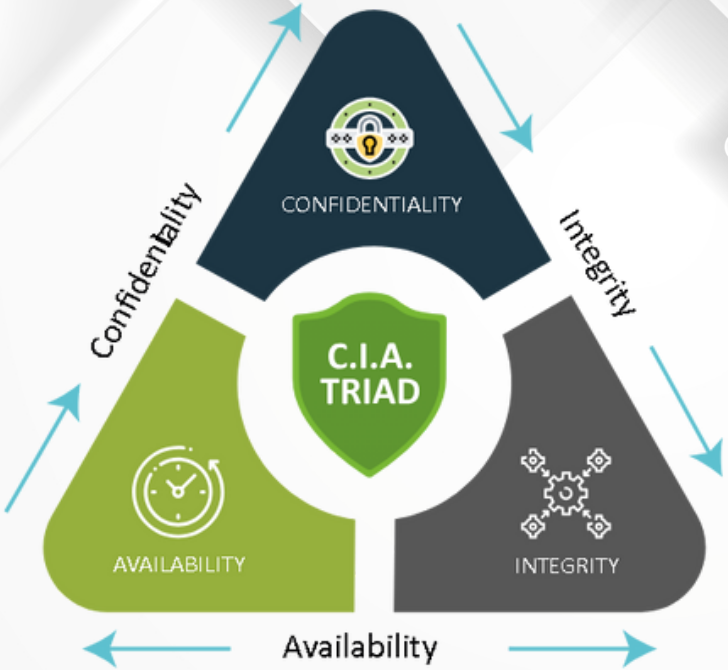
USE TRUSTED NETWORKS

- Use websites that has an "s" in https which stands for "secure".
- Avoid using unsecure networks.

THE DETERMINATION OF THE OPERATIONAL AND CYBERSECURITY STANDARDS WITHIN THE NPS (PSD-12)

The NPS industry should ensure that they implement measures to protect user information and transactional data from unauthorised access, tampering, and other security threats. All safety and privacy aspects of payments should at minimum be guided by and comply with PSD-12 to ensure data confidentiality, integrity & availability.

MS. ESTER NGWENA
Senior Analyst: NPS Policy & Data Analytics



CONFIDENTIALITY

PSD-12 requires appropriate protective controls to be implemented by NPS industry in line with best practice standards such as strong passwords and two-factor authentication.

INTEGRITY

PSD-12 requires encryption which converts payment instructions and customer information into a code that is only readable to the legitimate recipient, to prevent unauthorized access and changes.

AVAILABILITY

PSD-12 mandates that 2 hours should be the longest time a core banking system can be down after a disaster, to ensure systems are timely restored & available to consumers.

Ultimately, the role of information security extends far beyond dedicated IT or cybersecurity teams, **IT IS EVERYONES RESPONSIBILITY**. It is a collective effort that requires commitment and participation from everyone. By fostering a culture of security, being vigilant, and implementing the best leading cyber security controls, we can mitigate security risks and protect against emerging threats in today's digital landscape.

GET TO KNOW MORE ABOUT VIRTUAL ASSETS

Did You Know?

Unregulated virtual asset activities pose risks to the public, that include scams, security vulnerabilities, and investment losses due to platform failures, among others. To address these concerns and safeguard the funds of the public, the Virtual Assets Act, 2023 (No.10 of 2023) was promulgated in 2023. The Virtual Assets Act gives the Bank the powers to license, regulate, and oversee virtual assets service providers and related activities to prevent market abuse and protect the public.

WHAT IS A VIRTUAL ASSET SERVICE PROVIDER?

A Virtual Asset Service Provider refers to any business or individual that performs services or operations related to virtual assets (also known as cryptocurrencies, digital tokens, or digital currencies). They provide these services for or on behalf of another person. One example of a virtual asset service provider involves a virtual currency exchange platform. For example, Ester wants to buy some Bitcoin, a type of virtual currency, but she does not have an account on any cryptocurrency exchange. Ester can approach any virtual asset service provider that is registered in Namibia, which allows individuals to buy, sell, and trade various cryptocurrencies.

WHAT IS A VIRTUAL ASSET?

A Virtual Asset is a digital representation of an asset that: a) can be moved, stored, or traded online, b) uses technology like blockchain or similar, and c) can be used for buying things or investing but does not include digital versions of regular money (coins & banknotes) or assets such as stocks and bonds that are regulated by the laws of Namibia regarding securities or financial assets.

Example of a virtual asset is Bitcoin: Which is a type of digital currency that exists only on the internet. It is like regular money, but it is purely virtual. You cannot hold it in your hand like coins or banknotes. Instead, it is stored in digital wallets on computers or smartphones. Bitcoin transactions are recorded on blockchain technology, which makes them secure and transparent. People use Bitcoin to buy things online, send money to friends or family, or even invest in it like stocks, among other.

THE TYPES OF VIRTUAL ASSET SERVICES AND LICENSES

INITIAL TOKEN OFFERING

Is a type of fundraising mechanism where new tokens (virtual assets) are created and sold to the public to raise capital for the virtual asset service provider's projects or operations. This concept is similar to an Initial Coin Offering (ICO), but it can encompass a broader range of virtual assets beyond just coins, including tokens that represent utility, assets, or certain rights within a platform or ecosystem. This service is offered under the Token Issuer License.

EXCHANGING ONE VIRTUAL ASSET FOR ANOTHER VIRTUAL ASSET

This service is offered by a licensed virtual asset service provider to assist the public with the exchange of various virtual assets. For instance, if you want to swap your Bitcoin for another cryptocurrency like Ethereum, or vice versa, a licensed virtual asset provider facilitates such an exchange. This service is offered under Class "M" Virtual Asset Broker-Dealer License.

EXCHANGING VIRTUAL ASSET FOR FIAT CURRENCIES OR FIAT CURRENCIES FOR VIRTUAL ASSETS

This service is provided by licensed vitual asset service provider to make it easy for the public to exchange their virtual assets into Namibia dollars and other currencies and vice versa. This service is offered under Class "M" Virtual Asset Broker-Dealer License.

TRANSFER OF VIRTUAL ASSETS

This service is carried out by a licensed virtual asset service provider on behalf of another person or entity to move a virtual asset from one virtual asset address or account to another smoothly and securely. This service is offered under Class "O" Virtual Asset Wallet Services License.

A VIRTUAL ASSET EXCHANGE

This is a platform provided by a licensed virtual asset service provider to enable the public to trade different digital assets such as cryptocurrencies tokens etc. This service is offered under Class "S" Virtual Asset Market Place License.

If you are interested note the following:

- Only individuals or businesses handling virtual assets for others need to apply for a virtual asset service provider license. If you are trading cryptocurrencies for yourself, **you do not need to be licensed as a virtual asset service provider.**
- A virtual asset service provider operating as an individual, close corporation, partnership, trust or an entity must be **registered in Namibia and licensed by the Bank to offer virtual asset services.**
- Adhere to all other requirements listed in the **Ten (10) Virtual Assets Rules and Regulations** accessible on the Bank's website via this link.

Click the link *https://www.bon.com.na/Bank/Exchange-Control/Legal-Framework/Regulations.aspx*

WHERE CAN THE VIRTUAL ASSETS ACT BE FOUND?

The Virtual Assets Act is accessible on the Bank's website via the following link:
https://www.bon.com.na/Regulations/Virtual-Assets-Act-2023.aspx