Let’s Talk Cyber Security

The World Economic Forum forecasts that by 2022, over 60% of global GDP will be digitized and an estimated 70% of new value created in the economy over the next decade will be based on digitally enabled platforms.

In our part of the globe, we cannot afford to be left behind.

As we embrace more digital payments and move towards a more cash-lite payment environment, we reap the benefits of faster, easier and more convenient payment systems. We also reap the myriad of opportunities for business expansion and creation as new opportunities and business models are enabled.

However, in a digital environment, the issue of cyber security takes on a greater level of importance.

In the physical world, your money, household items and car keys, if not safely secured, can be stolen from your person or premises. Your signature can be forged or physical IDs tampered with and successfully used by an impersonator to access items that you value.

In the digital world, these crimes take on a digital form, but with the same sinister objective.

Ensuring protection from cyber-theft, cyber attacks and identity theft is not just the responsibility of software developers and programmers, or IT technicians and digital service providers, but it is also a responsibility for the end-user.

IT industry security standards and best practices are built into the DXCD solution to ensure maximum security of the DXCD environment. However, it is important that DXCD wallet users adopt basic cybersecurity measures that can improve the safety of their mobile devices and their DXCD app. Effective and efficient mitigation of cybersecurity risk has to be a shared responsibility and as the end user, you have an important role to play in ensuring the safety of your digital space.

When it comes to the DXCD, transactions would be enabled through a digital wallet app that you can download from the Apple and Google Play app stores onto your mobile smart device.

Cont’d on page 2
Here are a few steps that you must take to ensure that you play your part in securing your mobile smart device and your DXCD wallet app.

1. Create a strong password for your mobile smart device and your DXCD wallet app. For tips on creating strong passwords click here: https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

2. Never share your passwords with anyone.

3. Change your passwords regularly. Every 3 months is recommended.

4. Do not use access credentials (such as your password and security phrase) used in other applications as your DXCD wallet app access credentials. Once an attacker gets control of your credentials for one application, he/she will try to use them to access other applications that you own.

5. Embrace multifactor authentication as a security benefit. Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction: A password and a security question or a password and biometric information (e.g. iris scans, fingerprint scans, facial recognition). Multifactor authentication provides an additional layer of security and will be part of the DXCD wallet app architecture.

You are called to Own, Secure and Protect your DXCD wallet application and the assets associated with it. Answer the call!