"NICE TO CYBER MEET YOU" #SKELM

WISE UP. WATCH OUT. DEVICE AND SOFTWARE MANAGEMENT

MOBILE DEVICES AND TABLETS

- Secure your smartphone enabling the lock screen and security function, be it a pattern password or fingerprint screen lock.
- Where possible don't save any sensitive personal information and bank account details on your electronic devices.
- Think before you download apps to your mobile or tablet devices.
- Do not bypass built in security measures by "rooting" you device
- Only download mobile apps from secured and trusted sources
- Read the access requirements before you accepting the software installation (android permissions) of new apps.
- Install mobile security and antivirus software from a trusted security vender.
- Disable the "Sharing" function your mobile device if not needed.
- Enable the settings to remotely locate and factory rest your electronic devices.
- Keep your mobile device and antivirus software up to date with the latest security patches.
- Encrypt the data on your device where possible.

CONNECTIVITY

- Disable any wireless connection settings (e.g. Bluetooth, Wi-Fi and NFC) when you're not using it.
- Disable your push notification settings on mobile devices if not needed.
- After completing your transactions, ensure that you sign out of your Online Banking session and close your browser. If possible also power off your PC, this is especially important when you share the device with other people and at public locations
- Clear the browser cache on your PC and Mobile device regularly
- Do not log into a computer with administrator rights unless you must do so to perform specific tasks. (Practice the Principle of Least Privilege (PoLP).)
- Ensure that all personal Wi-Fi network are password protected and that all the necessary security settings are enabled.
- Do not use easily hacked security configurations like WEP, use the more recent and secure configurations.
- Avoid sensitive transactions on public Wi-Fi networks.
- Don't send passwords or account login credentials over public or unsecured Wi-Fi networks.
- Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password.

BEHAVIOUR

- Use strong passwords for all your accounts
- Change your password regularly and never share it with anyone else.
- Don't use any Personal Identifiable Information (PII) as a password, user ID or personal identification number (PIN)
- Be wary of email attachments and free software from unknown sources.
- Be mindful of how much personal information you share on social networking sites.
- Always set the privacy settings on your social media profiles to the highest level possible.

SabricZA @Sabric SabricZA

FOLLOW US ON SOCIAL MEDIA TO KEEP UP TO DATE

sabric

Making South African banking safe, secure and fraud free