Dear Valued Customer,

There is a new ransomware attack in circulation where the malware uses an attack that starts with a phishing campaign, getting a user to open an infected email through an attachment or embedded URL.

Once your computer is infected, your files/drives are encrypted and you are locked out of the whole system. The malware then informs you that the only way to decrypt your files and recover your system is to pay the cybercriminal a ransom (thus the name ransomware).

How to avoid being a victim of Ransomware?

- Always make use of a genuine/licensed operating system which is regularly updated
- Ensure your anti-virus is updated regularly
- Never open/click on any URL/link from an unknown sender or from any suspicious email
- Always use the latest web browsers versions

Important Notes

- Internet Banking Users should ALWAYS access SBM Internet Banking from SBM official website ONLY i.e. through https://www.sbmgroup.mu and by clicking on the Internet Banking link on the website.
- For any suspicious emails originating under SBM name/logo, customers are requested to call us on 207 0111 to ascertain genuineness of e-mails.

Of note, the Bank will never ask for password or other credentials from its clients.