Don't be a victim of cyber crime!

Understanding the dangers of malware

In 2019, an alarming 9.9 billion malware attacks were detected worldwide[1].
Here's how you can safeguard your personal devices and home network from
cyber threats.

What is malware?

Short for 'malicious software', malware is an intrusive programme installed on
your computer or smartphone, often without your knowledge or permission.
Once installed, it enables cyber criminals to commit fraud, like steal your
banking credentials, run payment scams or hijack your system for a ransom.

Understand the common types of malware

Virus: infects files and software, and spreads to other computers in the network

Spyware: spies on your online activities and collects your information

Ransomware: encrypts information and keeps it from you, in exchange for money

Trojan: disguises itself as a legitimate software to modify, destroy or steal

Bank safely with us

Malware can come from various sources, like fake Standard Chartered assets; including websites or emails with attachments containing malware. You can protect yourself from malware by taking these precautions.

Never download files (including email attachments) without verifying that they are from a legitimate source. To access our banking services or resources, visit our website at https://www.sc.com.

Delete junk and chain emails. If you have opened one, do not click on any links or download any attachments. To change your Online Banking password, use our i-banking site. Never change it via any email links.
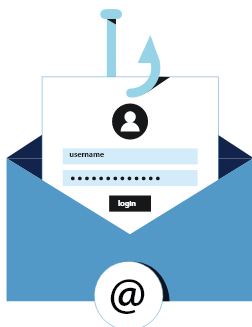
Install anti-virus and anti-malware protection on your devices. Enable the 'automatic updates' feature to ensure the software is able to detect and remove newer malware.

Never connect to unknown and unsecure Wi-Fi networks when carrying out online banking. If you are using your home network, ensure your router is secured.

We are happy to help you

Please reach out to our customer service hotline at 02-724-1553 immediately if you suspect any unauthorised access or transactions have been made to your account. We will stop all transactions to protect your account and you may be required to make a police report.

Together, we can STOP cyber crime.

For more information on malware, please visit https://www.sc.com/global/security-tips/

Here for good

Please do not reply to this e-mail.

You are advised not to send any confidential and/or important information to the Bank via e-mail, as the Bank makes no representations or warranties as to the security or accuracy of any information transmitted. The Bank shall not be responsible for any loss or damage suffered by you arising from your decision to use e-mail to communicate with the Bank. It is essential that prior to taking into consideration any information on this site, or responding to or sending any information or materials to us in response to this mailer, you have read and understood this Important Legal Notice.