standard chartered

Straight2Bank Security Features

Straight2Bank is a fully integrated and secure online banking platform, and we take protecting your finances seriously.

CYBERSECURITY MEASURES

Preventing Cyberattacks
We use smart tools such as Distributed Denial-of-Service (DDoS) mitigation tools to defend against cyberattacks that could disrupt your online banking experience.

Keeping Your Software Up-to-Date
We regularly update our systems with the latest security patches to keep you safe from new threats.

Data Protection with Encryption
We use advanced and industry standard encryption technology - Transport Layer Security (TLS 1.2/1.3) to protect your data when using Straight2Bank. This means all data, while traveling between devices and our servers, remain safe.

PREVENTING UNAUTHORISED ACCESS

Multi-Factor Authentication (MFA)
We offer an extra layer of security with MFA. This means you will need more than one factor to access your account, making it extremely difficult for anyone to get in without your permission.

Strong Security Walls
We have multiple layers of security (De-Militarised Zones) to keep your information safe from any unauthorised access.

ONGOING MONITORING

Detecting Suspicious Activity
Our advanced tools and security team watch for any unusual logins or activities, and they will send out an alert if something does not seem right.

Transparency with Audit Trails
We keep a record of your online banking activities for any future investigations.

RECOMMENDED ACTIONS & KEY CONSIDERATIONS TO ENSURE A SAFE AND SECURE ONLINE BANKING EXPERIENCE

Individuals
- Stay vigilant and avoid opening emails or clicking on links from unknown senders.
- Take control of your online privacy by managing your cookie preferences when accessing Straight2Bank.
- Ensure that you establish MFA/2FA for added security layer to access your Straight2Bank account.

Account / System Administrators
- Periodically review user access rights on digital banking platforms to make sure only those authorised have duly assigned access.
- Implement adequate segregation of duties and apply least privilege principle
- Set up notifications and alerts for unusual activities.
- Have regular training on fraud awareness and internal controls for all staff.

Technology & Cybersecurity Teams
- Enable Domain-Based Message Authentication, Reporting & Conformance (DMARC) which filters spam/phishing emails from reaching employees' inbox.
- Install latest anti-virus and anti-malware software.

Disclaimer

This material has been prepared by one or more members of SC Group, where "SC Group" refers to Standard Chartered Bank and each of its holding companies, subsidiaries, related corporations, affiliates, representative and branch offices in any jurisdiction, and their respective directors, officers, employees and/or any persons connected with them. Standard Chartered Bank is authorised by the United Kingdom's Prudential Regulation Authority and regulated by the United Kingdom's Financial Conduct Authority and Prudential Regulation Authority.

This material has been produced for reference and information purposes only, is not independent research material, and does not constitute an invitation, recommendation or offer to subscribe for or purchase any of the products or services mentioned or to enter into any transaction.

Some of the information herein may have been obtained from public sources and while SC Group believes such information to be reliable, SC Group has not independently verified the information. Information contained herein is subject to change at any time without notice. Any opinions or views of third parties expressed in this material are those of the third parties identified, and not of SC Group. While all reasonable care has been taken in preparing this material, SC Group makes no representation or warranty as to its accuracy or completeness, and no responsibility or liability is accepted for any errors of fact, omission or for any opinion expressed herein. The members of SC Group may not have the necessary licenses to provide services or offer products in all countries, and/or such provision of services or offer of products may be subject to the regulatory requirements of each jurisdiction. You are advised to exercise your own independent judgment (with the advice of your professional advisers as necessary) with respect to the risks and consequences of any matter contained herein. SC Group expressly disclaims any liability and responsibility whether arising in tort or contract or otherwise for any damage or losses you may suffer from your use of or reliance of the information contained herein.

You may wish to refer to the incorporation details of Standard Chartered PLC, Standard Chartered Bank and their subsidiaries by visiting the contact page of our website and view our locations.

This material is not for distribution to any person to which, or any jurisdiction in which, its distribution would be prohibited.