CMB London Branch On-line Banking Security Policy

20/09/2022

On-line Banking simultaneously brings us convenience and considerable risks. In this regard, China Merchants Bank London Branch (CMB London) has always placed the security of transactions and information first. Heavy security features in CMBL Corporate On-line Banking play a vital role in protecting the security of your account and monies. You can bank On-line with peace of mind.

On-line Security Firewall - the PC's Exam for Safer Internet Banking

You are strongly recommended to install an anti-virus software in your PC to protect your PC system from external On-line illegal attacks. Security firewall detects and removes spyware and system bugs on your PC and greatly mitigate the risks of your PC being attacked by spyware in internet and provide powerful safety protection to On-line Banking. To further protect your CMB London On-line Banking system, we provide you the Web Application Firewall and Application-Level DDoS Protection tools which can detect and monitor the On-line Banking security risk. We also use external independent experts to conduct Penetration Test annually to ensure the safety of our On-line Banking system. Please be aware of any suspicious signs when you turn on your PC. If you have any doubts about your PC’s on-line security, please don’t log into your On-line Banking system and speak to us.

On-line Banking Security Tool - Token

The On-line Banking Token is an On-line Banking security tool newly launched by CMB. The Token actually uses a dynamic On-line Banking password as an additional security measure to protect the monies in the account. In other words, your account is safe once the Token is kept

safely. Now you can use On-line Banking services with peace of mind. Please don’t share your Token with anyone else.

One new password each time, simple, fast, convenient, and safe. The password can be used in many situations when you log in to the system and make transactions. Having an "On-line Banking Token" on hand will stop Trojan virus, bogus mail and fraudulent website from entering your Internet Banking, protecting your best interests.

The On-line Banking Token is free. For further details please contact our Branch.

Unique Functions + Good Habits – Protect Customers Using Static Password

You should always keep security information safe, do not sharing it with anyone else.

Please note that you should always take precautions to protect against On-line frauds such as bogus websites or Trojan virus, by following the tips listed below:

◆ Log on the right website ◆ Protect My Password

◆ Ensure Computer Safety ◆ Deploy Other Protective Measures

Fraud Awareness

When you use our On-line Banking services, you are protected by our guarantee. This means that if you tell us a payment from your account was not authorised and ask us for a refund, we’ll reverse the transaction as soon as we can – though there are some exceptions to this.

For instance, we might not offer a refund if we think you have acted without reasonable care – by giving someone else your Log-in Password or Token, or by keeping your PIN written down in an unsecured place.

We can also refuse a refund if we think you are trying to commit fraud. We might involve the police in these cases.

Scam Awareness

A scam is where you are tricked into making or authorising a payment to a criminal's account. Scammers impersonate banks, retailers and official organisations using emails, phone calls and texts that look and sound genuine. Scammers are quick to adapt and are constantly creating new scams. Stay up to date on the latest scams. There are some pits for you:

- if someone contacts you saying they are from a bank and asks you to move money out of your account, put the phone down immediately – it's a scam as we will never ask you for this;
- if you aren't sure who the caller is, end the call, and call back on a number you know is genuine, like the number on our Website;
- if you get an email or text you were not expecting, don't open any links or attachments in it;
- Read the warnings that appear in your app and On-line Banking when you make a payment.

On-line Security System

We've put three lines of defence in place to make it harder for fraudsters to get through.

- Data encryption – our On-line Banking service is hosted on a secure, 256-bit encrypted server. This means that any information you send us is scrambled for your protection;
- Timed log out – we will log you out if you don't use the service for 10 minutes. This gives you extra protection if you forget to log yourself out;
- Deactivation of your log-in details – we'll automatically disable your access to On-line Banking if 3 incorrect log-in attempts are made. This is to stop fraudsters making repeated attempts to get into your accounts.

Fraud Monitoring

We are always checking for any suspicious activity on your account, so you may get a text message or call from our automated system to confirm a recent transaction or a change of address.

Sometimes, we may delay or decline transactions that we think are unusual, or even block your account until we can confirm that you are making the transaction. Keep your contact details up to date so we can get in contact quickly to keep any inconvenience to a minimum.

If we do call, we will never ask for your passcodes, passwords, PIN, Token details, Token Passcode or sensitive account information. We will never ask you questions by a text message; it is to notice you only.

Fraud Report

Fraud is a criminal act to deceive you and take your cash – it's a transaction that you didn't make or authorise.

If you think you have been targeted by fraud and have lost money, call us straight away. You should contact the Branch Relationship Manager immediately by email and phone call.

Once you have reported fraud, we will give you a case reference number. Make a note of this and keep it safe – it's confirmation that we've logged your case. Then we will investigate and contact you within 7 days to give you an update. If we do this by letter, it could take an extra 3 to 4 working days. We might send you a disclaimer form for you to fill in details of what happened - as part of your case. When you get this, fill it in and send it back to us within 10 working days. If we don't receive your form in time, within 10 days, we will close your claim – any temporary refund we have already given you will be taken back out of your account.