Security Tips

Contents

1 Internet Banking Security Tips

1.1 What we have done to protect you?

- With the use of 128bit Secure Socket Layer (SSL) encryption, we ensure the security of your data during transmission.
- Our system will monitor each login attempt. If there are several consecutive login attempts with incorrect password, the online service will be suspended immediately.
- We will not ask for customers' account number, password or any personal information via emails nor SMSes.
- Our web servers are protected by firewall systems to prevent unauthorized access.
- CCB(Asia) Online Enterprise Banking Services provide one-time password (OTP) or authentication token as one of your two-factor authentication tools for further verification when you need to conduct high-risk online transactions.
- We will notify you immediately once there is any high risk transaction carried out.

1.2 What can you do to protect yourself?

1.2.1 Password Protection

Password function is the key to your CCB(Asia) Online Enterprise Banking Services. It is important for you to safeguard your Customer Number, User Name, and Password. Please seriously consider the following suggestions:

- Destroy the original printed copy of your Password
- Change your initial password when you first access Online Banking Service.
- Change your Password regularly, recommended after 90 days
- Use a combination of numbers, upper and lower case letters for your Password
- Avoid using a number or name that is likely to or can easily be guessed by others, for example birthday, ID number or telephone numbers
- Do not use dictionary word such as "Password", easily recognized keypad patterns (qwerty, etc) that could be cracked by common hacking programs
- Avoid to use the same Password for different web service accounts and systems
- Never read out your Password over the phone
- Never disclose your Password to anyone, including staff at CCB (Asia)
- Never write down or record any Customer Number, User Name, and Password without disguising it

- Never include/send your Customer Number, User Name, and Password within an email message
- Ensure that no one is watching you while you key in your Customer Number, User Name, and Password
- Never leave your Security Device unattended to avoid unauthorized use of such device by third party to conduct online transaction.

1.2.2 Fraudulent Website

Fraudsters may send spoof emails pretending to be from China Construction Bank (Asia) Corporation Limited. Most of these emails or SMSes appear to come from the true source of the Bank.

Recipients of these emails or SMSes will be requested to input their personal information such as their username, password, credit card number, etc through these emails or SMSes.

Fraudsters through these emails or SMSes may instruct the reader to visit the fraudulent websites via hyperlinks embedded in these emails and request users to input their personal and account information.

Please be reminded that the Bank will NEVER ask customers to provide confidential data via SMSes, emails or hyperlinks, so do not respond to any suspicious emails or SMSes that request for such information or click on an embedded hyperlink/ QR code contained therein. You should delete them straight away.

How to prevent?

- Make sure you are connected to the Bank's official website at www.asia.ccb.com and/or m.asia.ccb.com for both desktop and mobile versions respectively before login or keying in any confidential data
- Do not access the website directly through hyperlinks embedded in e-mails. You should type www.asia.ccb.com and/or m.asia.ccb.com directly on the browser's address bar or access via a bookmark
- Verify the server certificate of our website (the locked padlock symbol in the web address bar of the browser)
- Update your anti-virus software and change your login password regularly
- Avoid login Online Banking with public wifi

1.2.3 Malware

Malware (malicious software) is a generic term for different types of malicious code. Examples of malicious code include computer viruses, worms, trojan horses, spyware & adware and ransomware. Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, and executing functions that a user never intended.

How to prevent?

- Do not use public computers or mobile devices to logon to CCB(Asia) Online Enterprise Banking Services.
- Do not download any programs or software onto your computer from suspicious sources, or click on the hyperlinks and attachments from questionable sources including malicious SMS or MMS messages.
- Install anti-virus and/or anti-spyware software programs in your computer and always run the programs before downloading programs or software or opening emails
- Regularly update your anti-virus and/or anti-spyware software programs and change your password
- Use the latest versions of operating system, applications and browser

1.2.4 Unauthorized Access

In order to protect your computer and its contents and to stop unauthorized access to your computer, you should:

- Install anti-virus and/or anti-spyware software programs, a personal firewall, and security patches on your computer
- Install and regularly update anti-virus/anti-spyware software programs and security patches
- Run the anti-virus/anti-spyware software programs before downloading programs or software or opening emails

1.2.5 Other Preventive Actions

Useful Security Tips to help you enjoy CCB(Asia) Online Enterprise Banking Services.:

- Remember to logout after you have completed your online activities
- Do not use shared computers to access your CCB(Asia) Online Enterprise Banking Services.
- Do not leave your computer and/or mobile unattended when you are accessing your web service account
- Check the date and time of your last visit to the CCB(Asia) Online Enterprise Banking's official website every time after you have logged in
- Review the transfer limit for non-registered third party account and lower it if necessary
- Be alert of the SMS notification sent to you after each funds transfer to non-registered account via Online Banking
- Never install uncertain applications provided by any third party
- Review regularly and follow security tips published by the authorities, e.g. The Hong Kong Association of Banks, Consumer Council, Hong Kong Police Force (Please refer to the Common Types of Technology Crime dated Oct 2020 https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/types.html), Hong Kong Monetary Authority, Securities and Futures Commission or Office of the Government Chief Information Officer, etc.

2 Public Website Security Tips

2.1 Password Protection

Password function is the key to your Online Banking and Bank By Phone services. It is important for you to safeguard your Password and PINs. Please seriously consider the following suggestions:

How to MAKE your Password safe

- Use a combination of numbers, upper and lower case letters for your Online Banking Password
- Avoid using a number or name that is likely to or can easily be guessed by others, for example, children's names, pets' names, birthday or telephone numbers
- Avoid to use the same Password for different web service accounts and systems
- Change your Password or PINs regularly

How to KEEP your Password safe

- Destroy the original printed copy of your Password or PINs
- Never disclose your Password or PINs or any details of the Password or PINs to anyone
- Never write down or record any Password or PINs without disguising it
- Never store your password on computers, mobile phones, or placed in plain sight

How to USE your Password safe

- Ensure that no one is watching you while you key in your Password or PINs
- Do not leave the computer midway without logging out of the online banking service
- Never read out your Password or PINs over the phone
- Never include/send your Password or PINs within an email message
- Under no circumstance, staff of CCBA never ask for your Password, User name

2.2 Fraudulent Website

What Fraudsters will do?

Fraudsters may send spoof emails pretending to be from China Construction Bank (Asia) Corporation Limited. Most of these emails appear to come from the true source of the Bank.

Recipients of these emails will be requested to input their personal information such as their username, password, One-time password (OTP), credit card number, etc. through these emails.

Fraudsters through these emails may instruct the reader to visit the fraudulent websites via hyperlinks/ QR code embedded in these emails and request users to input their personal and account information.

Please be reminded that the Bank will NEVER ask customers to provide confidential data via emails, so do not respond to any suspicious emails that request for such information or click on an embedded hyperlink/ QR code contained therein.

How to prevent?

- Make sure you are connected to the Bank's official website at www.asia.ccb.com and/or m.asia.ccb.com for both desktop and mobile versions respectively before login or keying in any confidential data
- Do not access the website directly through hyperlinks/ QR code embedded in emails, internet search engines or suspicious pop-up windows. You should type www.asia.ccb.com and/or m.asia.ccb.com directly on the browser's address bar or access via a bookmark
- Verify the server certificate of our website (the locked padlock symbol in the web address bar of the browser)
- Check the certificate information to ensure the certificate is issued to “www.asia.ccb.com” or “intl.ccb.com” and the certificate is still within a valid date.
- Update your anti-virus and/or anti-spyware software programs and change your login password regularly

2.3 Malware

What is Malware?

Malware (malicious software) is a generic term for a number of different types of malicious code. Examples of malicious code include computer viruses, worms, trojan horses, spyware & adware and ransomware. Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, and executing functions that a user never intended.

How to prevent?

- Do not download any programs or software onto your computer from suspicious sources, or click on the hyperlinks and attachments from questionable sources including malicious SMS or MMS messages.
- Install anti-virus and/or anti-spyware software programs in your computer and always run the programs before downloading programs or software or opening emails
- Regularly update your anti-virus and/or anti-spyware software programs and change your password
- Use the latest versions of operating system, applications and browser
- Do not use public/ shared computers or mobile devices to logon to Online Banking
- (Please refer to the Beware of Fraudsters https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/)

2.4 Unauthorized access

In order to protect your computer and its contents and to stop unauthorized access to your computer, you should:

- Install anti-virus and/or anti-spyware software programs, a personal firewall, and security updates on your computer and/ or mobile devices
- Run the anti-virus and/or anti-spyware software programs before downloading programs or software or opening emails
- Regularly update anti-virus and/or anti-spyware software programs and install security patches
- Keep your Username and Password confidential at all times
- Check the date and time of your last visit to the Bank's Online Banking website every time after you have logged in
- Remember to logout after you have completed your online activities
- Check your accounts from time to time and review alert messages and statements issued by the Bank in a timely manner
- Opt for SMS One-Time password (OTP) verification for accessing Online Securities Trading Services

Security Tips

2.5 Other Preventive Actions

Access Online Banking Services safely

- Avoid accessing Online Banking Services via public/ shared computers, and mobile devices or public Wi-Fi
- Check the date and time of your last visit to the Bank's Online Banking website every time after you have logged in
- Do not leave your computer and/or mobile unattended when you are accessing your Online Banking Services
- Remember to logout after you have completed your online activities
- Review the transfer limit for non-registered third party account and lower it if necessary
- The Bank does not affiliate with any third party aggregator mobile apps and customers should not disclose their online banking credentials to third parties
- Do not install any unknown third party aggregator app
- Use a reliable computer maintenance/repair service provider
- Customer should provide a valid mobile phone and contact number for notification purpose. If any of these numbers is changed, please notify the Bank timely
- Never install uncertain applications provided by any third party

Be aware of message from Bank

- Be alert of the SMS notification sent to you after each funds transfer to non-registered account via Online Banking
- If you have any suspicion or receive One-Time Password through SMS more than once, please contact us immediately
- Be alert of the messages the Bank sent to you and verify your transaction records
- Not to forward SMS One Time Password sent by the Bank to other mobile phone number
- If you suspect anyone else has accessed your web service or you have found any suspicious transactions, please call our Bank By Phone at 277 95533 or Credit Card 24-Hour Customer Service Hotline at 317 95533

Other related information

- To learn more about the e-leaflet of "Major Safety Tips on Using Internet Banking Services" published by Hong Kong Monetary Authority, please click here.
- To learn more about the publications published by The Hong Kong Association of Banks, please click here.

Peace of Mind Guarantee

Customers of Online Banking Service are protected against any third party fraud. You will not suffer any loss if money is withdrawn from your account without your knowledge, consent and authorization, provided that you have not acted with gross negligence, dishonestly, fraudulently or in a criminal manner, alone or with others. Any unauthorized transactions must be reported to the Bank immediately when you become aware of any actual or suspected security or fraud. The amount covered is limited to the amount illegally transferred from your account. We do not cover any other losses, including indirect, consequential or special losses, damages, expenses, legal fees or loss of opportunity. Please refer to the Terms and Conditions for Electronic Banking Services.

Ensuring maximum online banking security is a joint effort and your cooperation is equally important. Please ensure that you observe the following precautionary measures so you can benefit from our online security service to its fullest.

~~2.10~~2.6 Mobile Banking Security

Safe usage of QR Payment

- Stay vigilant and make sure that the QR code is from a trusted source before scanning.
- Verify the transaction details before confirming the payment and check your bank record when the transaction is done.
- The QR code generated for mobile payment services may have embedded your personal credentials. Therefore, you should only share the QR code with third party when necessary.
- If you need to show your merchant QR code in stores, for example placing it at cashiers, stay vigilant to prevent the QR code from being replaced or amended by third party

Beware of SIM Swap

- Be vigilant If you find that you are not receiving any calls or SMS notifications for unusually long time.
- Contact your mobile service provider immediate if you suspect you have fallen victim to SIM Swap scam.
- Protect your mobile service portal access to avoid fraudsters activate SMS forwarding service or enquire SMS content.
- Do not switch off your phone if you are receiving numerous unknown calls. This could be a ploy to get you to turn off your phone to prevent you from noticing that your connectivity has been tampered with.

~~2.11~~2.7 Security Tips for ATM Cards

Other related information

- To learn more about the e-leaflet of "Major Safety Tips on Using Internet Banking Services" published by Hong Kong Monetary Authority, please click here.
- To learn more about the publications published by The Hong Kong Association of Banks, please click here.
-
- Please be aware that you would be liable for the loss caused by stolen card, if you did not follow the abovementioned security tips and inform the Bank in a reasonable time manner, or/ and involve in fraud or serious negligence.
- Please check the relevant security advice provided by the Bank.