Benefits & Features

Our Internet Banking service gives you flexibility in managing your day to day banking needs. By choosing to manage your accounts with Internet Banking, you can take advantage of our wide range of time-saving online services, and access your accounts at anytime, day or night. With CBI Internet Banking, your bank is open to you 24 hours a day, seven days a week.

What can I do with Internet Banking?

You can manage your bank accounts online through the Internet.

You can do the following:

- View current balances of your accounts.
- Check overdraft limits and the status of your loans.
- Check your recent transactions and statements.
- Know if a cheque you have issued has been paid.
- Pay your monthly utility bills or setup Standing orders for automatic bill payments.
- Transfer money to other CBI and non-CBI bank accounts.
- Set up standing orders.
- Transfer money between your own Current or Savings accounts.
- Update your contact information.

Manage your credit card online.

You can:

- View your last statement, balance and available credit or cash limits.
- View any recent transactions which will appear on your next statement.
- Pay your credit card bill.
- Pay outstanding amounts automatically each month. Choose to pay either the minimum or full amount each month. This is useful when your bill payment is due while you are away on holiday.

You can also:

- Request for a Cheque book.
- Update the statement cycle for your accounts.
- Use a secure email facility to communicate with the bank for your banking needs.

We are constantly improving our services and features to deliver best Internet Banking facilities to you.

How to Register

It is easy to subscribe to Internet Banking with CBI. What you need to do is, submit a completed application to one of our Branches and collect the Security Token. You will be banking online in a matter of days.

How can I get an application form?

1. You can download the application form by clicking here, or select “Download Forms” from the menu on the left. You need to have Adobe Acrobat Reader in your computer to open this form. If the computer does not have Adobe Acrobat Reader, please visit Adobe to download the program.

2. Printed application forms are also available for collection in all CBI branches.

How do I complete the Application?

The Internet Banking application requires only a little information to be filled in. It requires your contact details, accounts to be linked and Identity proof. Please note that for the Identity proof, you need to provide details of one of the following documents:

1. Passport

2. Emirates Identity Card

It is a must to provide a valid email address. Please make sure that the email address provided is correct and only you have access to it.

You can contact our call center for any further assistance or clarifications in completing the application form. Please call 800 224.

Where to submit the application?

Completed application forms can be submitted to any CBI branch. Please see Branches Locater to find the nearest branch. You need to have the proof of Identity mentioned above along with the application form to submit for registration.

Please meet a representative at the Customer Service desk and submit your application. When the application is found to be in order, a Security Token will be given to you. You need this Security Token when you login to the Internet Banking Service.

How will I know when I can access the Internet Banking service?

The Bank will notify you when your Internet Banking User access is ready to use. An email will be sent to you confirming the registration. Email notification is sent within two working days from

the date you submit the application. If you do not receive the email please check in your email account to verify that it has not been delivered to your junk/spam mail folder. You can then contact our call center to follow-up.

Please see “Benefit & Features” for more information. You can find important tips for the safety of your Internet Banking in “Security Tips”.

First Time Users Instructions

This guide will help you to start using the CBI Internet Banking service. Following the acceptance of your application to register for Internet Banking, CBI will provide you a Security Token which is to be used when login in to the Internet Banking service.

After the acceptance of your registration, you will receive a confirmation email from the bank. This email will contain your User ID for login. To make sure that you receive the email confirmation and other important email communications from CBI, please add cbionline@cbi.ae to the address book of your email.

Given below is a step by step guide for using the CBI Internet Banking service for the first time and to activate your User ID.

What you need to start using the CBI Internet Banking service:

- CBI Internet Banking User ID which you will receive in a confirmation email from the Bank.
- Security Token issued to you after the acceptance of your application.
- A computer/laptop with Internet Connectivity.
- Microsoft Internet Explorer 5.5, or higher version of web browser.

How to start using CBI Internet Banking service:

STEP 1

Open your web browser and log on here.

STEP 2

Accept the terms and conditions for CBI Internet Banking service by clicking "Agree". You will be then directed to the next screen for first time login verification.

STEP 3

Enter the CBI Internet Banking User ID and the six-digit Token PIN in the relevant field. The Token PIN is the six-digit number appearing on the token screen. Click "Next" to create Internet PIN.

STEP 4

You need to create your own Internet PIN. The Internet PIN should be six-digit numeric only. Letters or other characters will not be accepted in the Internet PIN. Type a six-digit PIN for the New Internet PIN and Re-Enter New Internet PIN. Click "Submit" to proceed.

With this, you would have completed the first time login process and activated your User ID for CBI Internet Banking service. Now you can click ‘Login’ to start using the service and accessing your accounts. The online demo available on the website will help you to use the facilities available in CBI Internet Banking service. For further information and inquiries, you can contact our 24 hour call centre on 800 224.

Using the CBI Security Token

Protecting the integrity of our customers' financial information is our top priority. We have therefore introduced a superior level of online security by way of two factor authentication with the CBI Security Token.

With the CBI Security Token and the Internet PIN, CBI Internet Banking provides what is known as two-factor authentication. The PIN number appearing on the token and the Internet PIN which was created by the user will be needed to authenticate user login as well as for all financial transactions. This means, even if another person gets to know your Internet PIN or User ID, they will not be able to do anything without the Security Token.

Not all transactions need the Security Token

The token will not be required for some non-financial transactions. It will be used to authenticate some transactions where funds are transferred. Also transactions which involve changes to your account details require Security Token authentication. This will allow you to check account balances and move funds between your own accounts as easily as possible and with safety.

Using the CBI Security Token

When completing transactions, Internet Banking may prompt you to key in the Token PIN number appearing on the Token screen. The Token PIN is the six digit number appearing on the Security Token. This number keeps on changing every 60 seconds. A Token PIN once used, can't be used again for another transaction.

How the CBI Security Token works

The CBI Security Token is not a wireless device. It does not emit any radio waves, frequencies or infrared.

The CBI Security Token works by generating a PIN that continually changes. Based on information registered with the Bank's Token Management System when your CBI Security Token is assigned to you, it is possible to match these PIN with your Internet Banking profile when you transact online.

The CBI Security Token can be used with any computer and no special software is required.

Forgot Password

Forgot Internet PIN or Locked User ID, What should I do?

If you have forgotten your Internet PIN, you will not be able to access Internet Banking. When you or someone else try to login with an incorrect Internet PIN, the system will lock your User ID for security reasons. You will not be able to proceed with login to Internet Banking until a new Internet PIN is rest for your User ID.

What Should I do?

1. Please download the User Modification Request Form and print it. You can CLICK HERE to download the form.
2. Complete the form with your Internet Banking details and Tick the "Reset" option, as shown below.

Please sign the form and fax it to the CBI Call Center +971 (0) 6 568 4237.

1. CBI will enable your User ID to reset a new Internet PIN and an email will be sent to you confirming.
2. When you receive the email you can go to the "Forgot Password" link in the Internet Banking home page to reset a new Internet PIN.
3. Key in your User ID and the Token PIN in the relevant fields and Click "Next".
4. Next you will need to key in a New Internet PIN and key it in again for verification. Then Click on submit to complete.

If you need more clarifications you can contact CBI call center 800 224

Security Tips

CBI Internet Banking employs various security measures to ensure that your transactions and personal information are protected. However, as a customer you can play a big part in protecting your banking and personal information.

To help you secure your Internet Banking Service, we have developed a number of tips covering the areas of:

1. Password protection
2. Internet security protection
3. Login
4. Hoax emails

1. Password Protection

- When using the Internet, including Internet Banking, always try to use hard-to-guess passwords.
- Remember the golden rules of passwords.
- Ensure you are the only person that knows your user access, password and PIN.
- Notify CBI to disable your Internet Banking service immediately, if you become aware that your Internet PIN is known to or has been used by someone else.

When using the Internet, including Internet Banking, always try to use hard-to-guess passwords:

Passwords will protect your account only if they are difficult to guess. Don´t share your password, and don´t use the same password in more than one place. If someone should happen to guess one of your passwords, you don´t want them to be able to use it in a number of places.

Remember the golden rules of passwords:

1. Do not choose a password that is easily identifiable (for example, your date of birth, telephone number or any other number relevant to you).
2. Change passwords regularly, at least every 30 days. CBI Internet Banking requires you to change the Internet PIN every 90 days.

3. Do not give your password to anyone. Beware of unsolicited calls or emails requesting personal information or card numbers. CBI would not ask you to disclose your Internet PIN's or password information.

4. Do not write down your password, even in a coded language.

Ensure you are the only person who knows your user access, passwords and PINs:

To ensure you are the only person who knows your personal access information, any access to your computer and banking information should not be written down or accessible to other persons, even if you believe it is coded.

Do not disclose your Internet PIN or any password to anyone including a family member, friend or a staff member of CBI.

Notify CBI to disable your Internet Banking service immediately if you become aware that your Internet PIN is known to or has been used by someone else:

If you suspect that your Internet PIN has been revealed to a third party, contact the CBI Call center immediately to disable or to reset a new Internet PIN for your Internet Banking service.

2. Internet Security Protection

- Using Internet Banking in public places - staying safe.
- Is your computer and information protected from viruses? Ensure your virus protection software is always up-to-date.
- For more effective Internet protection, try using a firewall between your computer and the Internet.
- Is your computer security up-to-date? You should check your computer security on a regular basis and download the latest security upgrades.
- Be cautious! Do not open email attachments from unknown sources.
- Make sure your family members and/or your colleagues know what to do if a computer becomes infected.

Using Internet Banking in public places:

- Be wary of your surroundings and ensure no one is observing you when entering in your User ID or Internet PIN.
- Never click on links embedded within emails, rather enter the URL directly into the location/address bar.

- Ensure that there is a padlock symbol in the bottom right corner of your browser.
- Never click the "save my password/details" option sometimes offered.
- Never change security details such as your Internet PIN in a public place (ie libraries, Internet cafes, etc,.)
- Do not leave your computer unattended or idle for long periods of time.
- Always log out from your Internet Banking session when you have finished and close the browser.
- Always use computers that have anti-virus software installed.

Is your computer and information protected from viruses? Ensure your virus protection software is always up-to-date.

A computer virus is a program that attaches itself to another program, but changes the action of that program so that the virus is able to spread. Viruses range from harmless pranks that merely show an annoying message, to programs that can destroy or disable a computer altogether.

Anti-virus software is designed to better protect you and your computer against known viruses, worms and Trojan Horses. A Trojan Horse is a malicious program disguised as something harmless, such as a game or a screen saver, but in fact contains a hidden code that allows an intruder to take control of your machine without your knowledge.

Being protected means three things:

- Having protection on your computer in the first place.
- Checking for new Internet security protection software updates daily.
- Scanning all the files on your computer periodically including incoming and outgoing emails.

For more effective Internet protection, try using a firewall between your computer and the Internet

A firewall is a piece of software or hardware that filters all Internet traffic between your computer and the outside world. It works to either block or permit Internet traffic to and from your computer. You can use the Firewall to better protect your home or business computer and any personal information it holds from offensive websites, spam and unauthenticated logins from potential hackers. A Firewall is seen to be essential for those that use their computers online, especially through the use of a cable modem.

Is your computer security up-to-date? You should check your computer security on a regular basis and download the latest security upgrades

Security is essential in protecting your information on the Internet. To do this, check your software vendors´ web sites on a regular basis for new security upgrades, or use the automated patching features that some companies offer. The programs and operating system on your computer may have valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security on a regular basis.

Be cautious! - Do not open email attachments from unknown sources.

Email is one of the prime movers for malicious viruses. Regardless of how enticing the ´subject´ or attachment may look, be cautious. Any unexpected email, especially those with attachments (from someone you may or may not know), could contain a virus and may have been sent without that person´s knowledge from an infected computer. Should you receive an email of this kind and you are doubtful of its legitimacy, delete it.

Make sure your family members and/or your employees know what to do if a computer becomes infected.

It´s important that everyone who uses a computer is aware of proper security practices. People should know how to update virus protection software, how to download security upgrades from software vendors and how to create a proper password.

3. Login

- Ensure you login to the Internet Banking the correct way.
- Look for the ´padlock´ symbol at the bottom of your web browser.
- Do not leave your computer connected (online) when not in use.
- When viewing or using your personal information on the Internet, be aware of your environment.

Ensure you login to the Internet Banking service the correct way.

Always login to Internet Banking service by entering the website address www.cbiuae.com into the address bar.

Never access Internet Banking from a link in an email and enter personal details. If in doubt, contact the CBI Call Center.

Look for the "padlock" symbol at the bottom of your web browser.

When "login" or entering personal information, look for the "padlock" symbol at the bottom of your web browser. The "padlock" symbol indicates that the page you are on has additional security. You can double-click the padlock symbol to view the certificate´s details.

Do not leave your computer connected (online) when not in use.

When leaving your computer unattended, you should either shut it down or physically disconnect from the Internet connection. This reduces the risk of unauthorized access to your computer.

When viewing or using your personal information on the Internet, be aware of your environment.

Care should always be taken in unknown areas to prevent anyone from viewing your personal information, including when typing in your passwords or details of account numbers on the Internet.

Be cautious when accessing public computers or any computers you do not control.

4. HOAX EMAILS

What should I do if I receive a hoax email?

1. Delete the email

If you receive a hoax email, delete the email immediately. Do not click on any links and; do not open any attachments. Never provide personal details or sensitive information such as your PIN, password, customer registration information or other log on details.

CBI does not send emails requesting personal or account information.

2. Report the incident

Please inform us if you happen to get any hoax email.

3. Scan your computer for viruses

Many hoax emails contain viruses or Trojan Horses (key logger), which are downloaded to your computer when you open any attachments or select any included links. If you have clicked on any items within the email, run a complete virus check of your computer. We recommends that you perform virus scans on your computer regularly.

4. Reset your Internet Banking PIN

After scanning your computer and ensuring it is free of viruses or Trojans, reset your Internet Banking PIN.

I don’t have anti-virus protection.

Computers without anti-virus protection or out-of-date anti-virus programs are vulnerable to future attacks by malicious software like viruses or Trojans. Anti-virus programs are a simple and inexpensive way to protect your personal details from these threats.

A number of different vendors provide complete suites of Internet security software.

We recommend that you do not use Internet Banking until you have up-to-date anti-virus protection.

I received a hoax email from another financial institution.

Hoax emails can imitate any organization or financial institution. You may receive emails imitating organizations that you have no affiliation with.

If you receive a hoax email claiming to be from another organization or financial institution, delete the email immediately and scan your computer for viruses. Do not click on any links or open any attachments.