Benefits & Features

CBI's Corporate Internet Banking – Inquiry Services gives you the ability to view account details and transactions anytime, anywhere.

What can I do with Internet Banking?

You can inquire on your bank accounts online through the Internet.

Account / Cheque Services:

- View current balances of your accounts.
- Check your recent transactions and statements.
- Know if a cheque you have issued has been paid.

Card Services:

- View the last statement and balance with available credit limits.
- View any recent transactions which will appear on your next statement.

We are constantly improving our services and features to deliver best Corporate 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?

You can get a copy of all forms relating to Corporate Internet Banking – Inquiry Services by contacting your respective Relationship Manager.

How do I complete the Application?

If your company wants to avail of the Corporate Internet Banking – Inquiry Services, the following original documents are required to be provided to CBI.

1. Corporate Internet Banking – Company Registration form with a Letter of Mandate attached
2. Corporate Internet Banking – User Registration form with Indemnity document attached
3. Identity proof (Emirates ID / Passport with Resident visa)

Your contact details and accounts to be linked for Corporate Internet Banking online view needs to be filled in the application form. Please ensure that the email address provided for user and Company Contact person is correct. Notification for successful Corporate Internet Banking registration will be sent to the company contact person.

You can contact our respective Relationship Managers for further assistance or clarifications in completing the application form.

Where to submit the application?

Completed application forms can be submitted to any CBI branch. Please see Branches Locator to find the nearest branch.
Please meet a representative at the Customer Service desk and submit your application in person.

How will I know when I can access the Corporate Internet Banking – inquiry services?

The Bank will notify the company contact person via an automated email notification when your registration for Corporate Internet Banking – Inquiry Services is completed. The email will be sent to the company contact person within three working days from the date of submission of your original application forms.

Please ensure to check junk/spam emails folder in order not to miss the email. Still, if you have not received the email, please contact your respective Relationship Manager for follow-up.

Please print out the email notification and attach it together with the filled in Token Acknowledgment Form. Submit both together in the branch along with proof of identity. Once submitted, the branch representative will provide you with your Security Token. You need this token for first time log in to Corporate Internet Banking – Inquiry Services. Please wait for two working days after receipt of token before you do first time log in.

You can find important tips for the safety of your Internet Banking in “Security Tips”.

First Time Users Instructions

This is a step by step guide for using CBI's Corporate Internet Banking – Inquiry Services for the first time.

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

- CBI Internet Banking Company Login ID and User Login 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.
- Acrobat Reader 8.0 or higher version
- Microsoft Excel 97 or higher version

How to start using CBI Internet Banking service:

STEP 1

Open your web browser with https://cbionline.cbi.ae and select "First Time Login" under Corporate Internet Banking menu.

STEP 2

Accept the terms and conditions for CBI Corporate 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 Company Login ID, User Login 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 Login ID for CBI Corporate Internet Banking service. Now you can click ‘Login’ to start using the service and accessing your accounts.

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 (once these are made available). 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.

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 Corporate 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 fill in the Password/Token Reset Form and submit it to the branch for verification.
2. CBI will enable your User ID to reset a new Internet PIN and an email will be sent to you for further action.
3. 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.
4. Key in your Company Login ID, User Login ID and the Token PIN in the relevant fields and Click "Continue".
5. 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 on 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.