



CyberCulture

Internet Usage Culture



بنك قناة السويس
SUEZ CANAL BANK

19093
www.scbank.com.eg



Dear Customers,

Some believe that freedom of the Internet is so recognized that some may forget that this freedom itself may cause loss of privacy. Since the internet is attached to our daily lives, it became necessary to increase the awareness of protecting yourself and your information when you use and surf the internet or what we call the "World Wide Web".

Here are some common inquiries and their answers:-

Is there someone monitoring me closely on the internet?



Yes, the possibility exists. Everyone must know that the security authorities in the countries who own giant internet servers and allow us to use it, record all the activities on the internet by all possible means on giant databases

They used specialized programs to analyze such data and transfer it to information - which is the basic goal behind incurring the cost and management of these servers. They can also monitor the data of certain personal computers and obtain data from the communications companies indirectly.

Is your privacy breached while surfing the internet?

It is never sufficient to trust websites, browsers or internet providers to do this for you. In fact, you should stop trusting them because the default privacy settings of these services lack the required security. Each internet browser sends an HTTP cookie which is also called (Cookies) to the computer.

These cookies give information about the pages which have been visited. Many of the websites - which we visit - leave these cookies on the computers and when we visit this page again, the site recognizes us, the times we visited the site and perhaps the places from where we use the computer. Advertisements of companies about the pages which you visited or information about a certain product you were about to search for can appear online. By evaluating this information, the web browser shows the ads that may fit my requirements. Although, you should know that cookies could be removed, we will shed a light on the aspects of protection that may be associated with the cookies in coming awareness booklets of information security.

Is there anyone else who has access to the pages I visit on the internet?

Many of the websites use the program of "Google Analytics" to gather more information about the behavior of browsers' users. This program transfers all the data obtained to Google Inc. Therefore, Google Inc. obtains many information from various sources and is able to compose a specific file for each user.

What happens if I use the Wireless LAN (Wi-Fi) in a café or airport to access the internet?

The Wireless LAN (Wi-Fi) is an insecure internet port and therefore the café's owner, any intruder, or the provider of this service can easily recognize all the pages, which was visited by his clients.



Does this apply on social networks?

The information that gathered by social networks is endless. A user's account on social networks remains opened all the time although he browses other sites. If a Facebook user clicks the button of "Like", all the information exists in the cookies transferred directly to Facebook. This way, Facebook also obtains information about the pages, which we visit on the internet.



Social Engineering Techniques:-

Social engineering is simply the art of access to sensitive information about computer systems or personal data or passwords from the users' systems. This is often by persuading users that the speaker is a person authorized to obtain this data. For example, this person makes a telephone call, tries to introduce himself/ herself, and convinces you that he/she is a representative of the bank and discusses with you some special details and confidential information of your bank accounts.

The trick may also take the form of an e-mail from an unknown source and to master the fraud technique the hacker attempts to gain the trust of a user and urge him/her to download the malicious file included in the message by many ways.

Including for example, Sending an attached file in the form of an (Excel) table entitled (How to calculate the Zakat upon money) or a request to (update Acrobat Reader programs) "Adobe Reader", etc.,.,.,.




Once the user downloads these files on the computer, a hidden program being operate on your own computer and encrypts all the files in it and they become blocked. The hidden program also changes the name of each file for not recognizing it, then the hacker sends a message to the user to blackmail him/ her financially and asks him/her to pay an amount of money in an account specified by him/her so the user is able to retrieve back his/ her own information.

Password:-

The password is the key of your internet account. Avoid using the same password for different systems. This is important, if you do so; you increase the risk of being vulnerable and penetrated by hackers, which could put your money also at risk. Someone may discover your password for this reason, so we strongly recommend that you use a different password for each system while making sure that they are strong ones (not less than eight characters, upper and lower case letters, numbers and special characters such as \$ or # or %)

You should also keep in mind the following when selecting a strong password:



-  It should be unique – avoid using the same password in any other services.
-  It should not be personal – do not use a password that can be easily guessed such as; the names of your children or wife or animals or dates of birth or phone numbers.
-  Do not ever write it – we strongly recommend not write or record your password. If you do not have other options than writing it down, try to write it or record it in a way that makes it incomprehensible for any other person.

Secure Internet

Kindly be informed that "Suez Canal Bank" staff will not call you to know your personal confidential details such as your personal identification number (PIN), Telephone PIN, Password or the three numbers on the back of the credit card. In case of receiving any phone calls asking for your personal information, please do not give any of your information and immediately contact our customer service center on the following number: **(+202) 19093**

Protection Modes:

When you access the bank's website, it shows that it is secure. You can know whether a website is secure or not if it begins with **https** or the key guard icon appears beside the link address in green color as per the following figure:



Encryption:

Encryption technology (SSL) used when accessing bank information to encrypt your personal information and make it secured before leaving the computer to ensure that it not read by any other person

As per the browser settings, a pop-up page will appear to tell you that you have accessed a page that is protect. The encryption process transfers your own data to the form of codes before sending them to the internet and by this way the unauthorized internet users are not allowed to view such data. In Suez Canal Bank, we use secured encryption layers that are compliant in accordance with the encryption standards.





Break time in protection mode:

If you forgot to close the web page and logged out of the website after accessing your bank information or if the computer becomes inactive for a period time during the protection mode, our system will automatically close and log out of the page. Although, we advise you to close the page once you finish browsing.



Technology

We use many protection layers and of course they cannot be fully disclosed, but the following means are perfectly used:

-  Anti-virus software are updated regularly;
-  We use multiple barriers to prevent access without permission;
-  We have secure information centers;
-  All the operating systems are regularly updated with the latest protection files.

Privacy of identity data

We use passwords access data we can use Assistant Authentication Devices (Token) and one-time passwords to be sure that we are dealing with you. Access to your own account is possible only in case of confirming your identity and using your correct name and password registered at the bank. For this reason, it is important not to disclose your password to any person and secure your assistant devices in your possession, which used to confirm the identity of your mobile phone or Token.

Automatic lock-down

After a number of incorrect attempts to login, you will not be able to log into your account. You should call the bank's call center in order to re-activate your account again.



“ Protection on the internet is a personal responsibility and duty ”

In addition to these procedures of protection, you play an important role in protecting your personal information since there are many things that you can do to protect yourself while connecting to the internet.

To start with, you should follow the significant rules mentioned previously along with the following rules:

Please keep in mind these important details

- Keep your personal data confidential
- Keep your password confidential
- Keep your personal computer and mobile phone protected
- Keep the authentication devices in your possession
- Make sure of the protection mode when you log into your account on the internet
- Keep your email confidential
- Keep your information confidential even when you're not connecting to the internet
- Do not be influenced by opening links from unknown sources to avoid being a victim of "E-Phishing" attacks and thus injecting your device with malicious codes
- Downloading and installing anti-virus systems and anti-malicious files on your smartphones and particularly when you use wireless networks;
- Closing the Wi-Fi and Bluetooth features on your devices while being in public places.













**Here are some
threats and
what should we
do about it..**

Counterfeit Websites:

There are fake websites that look like original ones and designed by forgers to attract a number of people to these websites through phishing emails and they always ask for confidential personal information.





What should we do?

-  Make sure that you are connected to the official website of "Suez Canal Bank" which is www.scbank.com.eg before entering any personal data.
-  Do not log into your bank account directly through links provided to you via email
-  Write the website name www.scbank.com.eg at the browser address or access through the desktop mark.
-  Try to check out the icon of lock-down (protection / key guard shape) and that it is in green color
-  Make sure that the browser protection mode is set by "Suez Canal Bank" through checking the issue date on the Certificate of confidentiality and protection 
-  You should change the password that you use to log into your bank account regularly.
-  Before downloading our apps from online stores, always check that the names of our apps are accurate and authentic.

Phishing:

This happens when the fraudsters send insidious messages randomly. These messages appear to be sent from legitimate source such as "Suez Canal Bank" and they may ask you to confirm some very significant information such as your account number, password and PIN number.

What should we do?

-  Do not do anything unless you are fully sure of the legitimacy of the sender and the request itself.
-  Be sure that "Suez Canal Bank" will never ask customers to give any important confidential data about their bank account through e-mails.
-  Do not reply to messages that ask for this information and do not click any links included in any of these messages.
-  You should update the anti-virus software and change regularly the password used to log into your bank account in order to keep and protect your personal data.

Insidious softwares that threats your computers:





Computer virus: A computer program that linked to other software or data files in order to execute it maliciously

Worms: An independent computer programs that copy themselves from one computer to another through the network.

Trojan horse program: A program that seems to execute certain actions, but when it starts, it performs other actions that harm information systems.

Spyware: A computer program that download secretly on your device online and record each click on the keyboard to know passwords and serial numbers.

What should we do?

-  Download ant-virus software, firewall and security packages.
-  Always run anti-virus software before downloading any other programs or opening any e-mails.
-  Do not open any link or download any attachment from untrusted sources.
-  Update your anti-virus software and change the password of your bank account regularly in order to protect your personal data.

CyberCulture



Internet Usage Culture



بنك قناة السويس
SUÉZ CANAL BANK

19093
www.scbank.com.eg