


Do you transfer money, make savings deposits or trade in securities over the Internet?

With Leumi's advanced security measures and by complying with a number of simple rules, you can undertake all these more securely.

 Leumi makes a constant effort to preserve the privacy of browsers and the confidentiality of banking information using the following measures:

- Adapting advanced means for securing browser operations.
- Upgrading and adapting security systems to current Internet threats.
- Strict inspections of all the systems by appropriate external bodies.

For your convenience we have summarized the major rules and measures for safe browsing:

- Typing the bank's URL and avoiding accessing the website through links or electronic mail messages (in order to avoid phishing).
- Ensure that, at the beginning of the URL, the letters https, which indicate coded communication, appear.
- Select a random password that is difficult to guess.
- Do not furnish any other body with your personal password even if it identifies itself as Bank Leumi or as being identified with it.
- Do not keep identification details in an exposed place, accessible to others or on the computer, in order to avoid their exposure by Trojan Horses or shareware, which enable access to files on the computer (see the report in Maariv).
- Do not send your identification details for accessing your personal account, including credit card numbers by electronic mail.
- When accessing the system, the date and time of your last communication with the system will appear. Thus it will be possible to ensure that the data that appear are indeed correct and that there has not been any unauthorized access to your account.
- While browsing the system, prevention of physical browsing of other bodies to the station from which the browsing is being executed.
- On terminating the use of the system, disconnect from the system using the exit action and, if using a random computer, closing the browser is recommended.
- Avoid browsing on computers with unknown security levels.
- Conduct a regular and frequent follow-up of your account on the Internet.
- Please note: Leumi does not usually send e-mail messages asking you to login to your account via an attached link. Should you receive an e-mail message that arouses your suspicions, do not click on the link that appears therein. Notify the support center immediately and send a copy of the notice to abuse@bll.co.il

General cautionary measures to adopt when using a PC

- Use information protection software such as: Personal Firewall, antivirus and anti- spyware software. Update these programs regularly.
- Update the operating system, browser and other shelf software with the adjustments published from time to time, that relate to the issue of information security.
- Avoid shared folders that contain personal files, while using shareware.
- Avoid installing unknown software and downloading files from unknown/unreliable sources on the Internet to your computer.

For further information, questions and support please contact the support center

- Member registered with "Glisha Yeshira", please call: +972-3-954-4333
- Member registered with "Leumi Premium", please call: +972-3-954-4888

Instructions for Browsing Your Leumi Account

While the Internet provides many diverse services, it conceals a number of risks. Therefore, we perceive great importance in preserving the basic rules for safe browsing.

Safeguarding Identification Details

- You identification details for the system are private and confidential. Do not give them to any other person or keep or save them in a disclosed manner.
- When identifying yourself to the system, make sure that there are no on authorized persons around you.
- Never give your personal password to any other body, even if it identifies itself as Bank Leumi or as being identified with the Bank. If, indeed you are asked to furnish your personal password, do not do so! Report this immediately to the supervisor of the support center.
- Do not keep your identification details on your computer for fear of their exposure by Trojan Horses or shareware files (such as e-Mule and Kazaa), which enable access to files on the computer.
- When registering for other websites, do not use the same identification details (username and password) that are used for identification at Leumi.

Accessing the System

- When accessing the bank's web site, type the URL yourself (www.leumi.co.il).
- When browsing to your account, make sure that the identification page URL begins with <https://hb2.bankleumi.co.il>, which is proof that this is the real address of the web site for browsing to the bank account.
- Browsing to your account is executed in a secured environment. Make sure that the letters https appear at the beginning of the URL, which indicates an encoded communication, compared with http, which indicates a regular communication.
- At the time of identification with the system and while working regularly with the system, make sure that the website pages are coded (SSL coding): when the communication to the bank is encoded, in Internet Explorer 6 an icon of a closed golden lock will appear at the bottom of the screen (see example). In Internet Explorer 7 the icon will appear in the ruler at the top section of the screen (see example).

Examples:

The Internet Explorer 6 security icon:



The Internet Explorer 7 security icon:



Working with the System

- When accessing your account, the date and time of your last communication with the system will appear. Ensure that the data that appear are indeed correct.
- During regular work with the system, avoid the physical browsing of other bodies to the station from which the browsing is being executed.

Verifying the Leumi Website on the Internet

- At the beginning of communication with the website, ensure that the site's general form and external appearance are, indeed, familiar to you.
- On browsing to your account, make sure that you have reached the Bank's secured website (direct browsing / Leumi Premium), by viewing the VeriSign confirmation. In order to view this confirmation, click on the orange VeriSign icon, allocated on the axis screen to your account (see example). You will then receive a page presenting the confirmation.



Example of the VeriSign icon:

- Alternatively, you can double-click on the yellow lock and a certificate issued by VeriSign will be presented, which includes the validity dates of the certificate. If you do not receive a notice certifying Leumi's identity, notify the support center immediately and work according to its instructions.

Sample of confirmation certificate:



Exiting the system

- After 20 idle minutes on the system, the connection will be terminated automatically at the system's initiative. However, on competing use of the system, do not wait for automatic disconnection and execute an initiated disconnection using the exit procedure.
- On terminating use of the system, especially on a random computer, you must close the browser. After exiting the system, accessing the system will only be possible by means of re-identification.

Treatment of Passwords

- Choosing a password – On first accessing the system, you have to feed the initial passport that you received and immediately replace it with your password. It is important that the password that you choose should be random, difficult to guess and easy for you to remember. The password should include at least six characters that include letters and numerals.
- Changing the password – The personal password can be changed at any time and it is recommended to change it whenever there is a fear of disclosure. In order to change the password, click on the "settings" button in the activity row in the upper menu. In the window that opens select "change password."
- Towards the end of 180 days from the first time that your passport was changed, the system will present you with a warning notice to change the password. If the password is not changed by the end of 180 days, it will be blocked.
- A blocked password – The password will be blocked after five unsuccessful typing attempts.
- Clearing the password – In order to clear a blocked password, contact the support Center at one of the telephone numbers recorded in the bank's books.

Working with a CD-ROM/Floppy Disk, Disk on Key while Executing Transactions

- An examination of the CD-ROM/floppy disk, is intended to reinforce the identity of the executor of the transaction.
- An examination of the CD-ROM/floppy disk at the time of executing the transaction is executed in cases in which the work is defined in this configuration. The default is executing a transaction without examining the CD-ROM/floppy disk.
- There is a unique key in the CD-ROM/floppy disk. When executing transactions, the system examines and verifies the existence of the unique key. If the examination is in order, the system allows work to continue and replaces the key with a new key. Alternatively, a message that the CD-ROM/floppy disk has not been identified and that the transaction will not be executed is displayed.
- [For further details regarding the issue of working with a CD-ROM/floppy disk](#)

Working with Cookies

- The cookies are encoded at a high level
- The cookies do not include your personal details

Instructions for Securing the PC

Instructions for Securing the PC

- Use an antivirus on the computer and update it regularly.
- Use anti spyware software for identifying spy ware on the computer and update it regularly.
- Use a Personal Firewall on the PC.
- Update of the operating system, browser and other shelf software with the adjustments published from time to time, related to the issue of information security.
- Do not keep your identification details on your computer for fear of their exposure by Trojan Horses or shareware files (such as e-Mule and Kazaa), which enable access to files on the computer.
- Avoid installing unknown software on your computer.
- Avoid downloading files from unknown sources on the Internet.
- Avoided opening additional Internet widows simultaneously with connecting to the system.
- We recommend defining the erasure of temporary files automatically on closing the browser through the tools menu > Internet Options > Advanced > Empty the Temporary Internet Files folder, when closing the browser.
- It is recommended to avoid browsing to your account from computers on which the security level is unknown.
- When exporting data and saving them in files on the computer, it is recommended to encode the files using the encoding tool.

Instructions for wireless network users

- Change the user name and password defined as the default on the wireless router.
- Securing the wireless communications using a wireless encoding protocol such as WPA.

Cautionary Measures against Internet Fraud

Similarly to many other global financial bodies, Leumi is targeted for attempts at fraud by hostile bodies. These bodies activate sophisticated methods for the purpose of collecting data on customers for the purpose of accessing their accounts. One of these methods is transmitting electronic-mail (e-mail) messages, which contain a link to false websites. This threat requires adopting cautionary measures by both the bank and its customers.

Following is a list of rules and recommendations, which would assist you in safeguarding and protecting private details that you use for browsing the Leumi websites:

- It is recommended to type the banks URL directly and not to access the site through links.
- When first accessing the website, ensure that the general form and external appearance of the website are familiar to you. Similarly, take note of the language used on the site. If you are used to logging in to your account though instructions provided in Hebrew, avoid feeding your identification details on a screen written in a different language.
- When using Internet Explorer 7, when the website is suspected of being false or when it is known to be a false site, the URL will appear against a red or yellow background with a warning presented alongside it.

Example



A website known to be false – colored red



A suspicious web site – colored yellow



Nevertheless, even if no warning signs about the browser appear, one must remain aware of suspicious signs.

- Under no circumstances should private details (username, passwords, account number, credit card number etc.) be transmitted to any other person through the e-mail, even if it identifies itself as Bank Leumi or as identified with the bank.
- Whenever accessing the web site through a link that appears in an e-mail message, ensure that you indeed have arrived at the Leumi website (see the section "verifying the Leumi website on the Internet" in the section Instructions for Browsing through Your Leumi Account). Fraudulent activities often involve false web sites, which appear to be precise copies of the official bank's website.
- Please note: Leumi does not usually send e-mail messages asking you to login to your account via an attached link.
- Should you receive an e-mail message that arouses your suspicions, do not click on the link that appears therein. Notify the support center immediately and send a copy of the notice to abuse@bll.co.il
- If you have accessed an aforementioned link and fed your identification details, login to your account immediately via Leumi's official website and change your password immediately and review the recent transactions that were executed since feeding your details as aforementioned. It is also recommended to change your user name at your branch.
- Please note: when feeding/transmitting your personal connection to Leumi details (including passwords), ensure that these web sites are included in Leumi's official web sites.

Signs of Fraudulent and Notices

- E-mail messages that expressly request transmitting identification details by e-mail.
- Messages that contain a note of urgency, which pressure you to furnish or update your registration details at the bank (either through e-mail or prima facie through the bank's website), while threatening impairment to the service should you not comply with the request.
- E-mail messages that contain grammatical errors (these errors assist the messages to bypass content filtering mechanisms that usually exist in large companies).

Leumi's Advanced Security Measures

Leumi implements advanced security measures into its systems for safeguarding your transactions and maintaining your privacy and the confidentiality of data and information at your disposal.

The Primary Measures

- **Identification on accessing the system** – Identification by means of three parameters: user code, personal password and identification field.
- **Database** – The bank's computer and database are not connected to the Internet directly and browsing to customer data is protected by means of an advanced information security system.
- **Encoded communication** – Transferring information between the bank's computers and your computer, via the Internet, is performed using encoded communication (SSL. at a 128 bit level).
- **Registration as a true website** – the bank's websites are registered at the American company VeriSign as secured websites, which contain a mechanism that enables contacting VeriSign as a third, independent body for receiving confirmation that reference is to the bank's official websites.
- **Protection components** – A variety of filtering components at the communications level (Firewalls etc.) and protection, and filtering infrastructure and applicative components.
- **Transaction journal** – Saving details of events related to uses of the system.
- **Inspection and monitoring** – Constant inspection and monitoring measures for communications with the website are activated.
- **Reporting** – the system reports any attempted intrusion into the Bank's control system
- **Inspection of information security** – Strict inspections of the system and its components are conducted by external bodies that specialize in this field.
- **Physical protection** – The servers are installed at Leumi. The server station is secured and protected against unauthorized bodies.

Measures for Securing Personal Leumi-Mail Message

The Primary Measures for Securing Personal Mail Messages – Leumi Mail

- **Encoding personal mail messages** – After selecting the desired message and clicking on the “save” button, a notice enabling you to choose whether you wish to save the file on your PC by encoding it or not will be presented. If you choose the option of saving by encoding, an encoded exe file will download on your computer in a strong coded algorithm (Triple Des).
- **A personal password for viewing the data in the file** – Viewing the data in the file is only possible after typing a personal password. After typing the personal password, an HTML file will open in which to present the data of your personal mail.
- **The date and time of opening /downloading postal mail to the computer** – Three dates appear for each mail message: “Sent on” – the date of sending the mail message from Leumi’s central computer; “Opened on” – the date the mail message was opened; “downloaded to the computer” – the date in which the e-mail message was saved on your computer. Ensure that the data appearing on the opening and saving dates of the mail message are indeed correct.
- **Using a public computer station** – While working at a public computer station that is connected to the Internet do not execute downloading and saving of mail messages at the station. Only view mail messages

Working with a disk/floppy disk


Inspecting a disk/floppy disk while executing transactions, is intended to verify that the execution of the transaction was executed by you (the owner of the floppy disk) only from your computer (when working with a disk). There is a unique key on the disk/floppy disk. When executing transactions, the system checks and authenticates the presence of this unique key. If the inspection is normal, the system allows work to continue and replaces the key with a new key. However, in the absence of this, the system gives a warning that it does not identify the disk/floppy disk and that the transaction will not be executed.

 You have the option of deciding which mode you wish to use when executing transactions:

- Executing transactions without inspecting the floppy disk.
- Executing transactions with the floppy disk with involvement of a third-party only (as for those entitled to transfer to third parties).
- Executing transactions with a floppy disk in all types of transactions.

 To change the man of executing transactions:

- Click on the "settings" buttons. In the transactions row in the upper menu and, on the page that opens, select the "executing transactions with a floppy disk" option.
- At the top of the screen, the current status of the disk/floppy disk inspection will appear. If you wish to change the status you must select the required option and click OK.

 Additional instructions

- Remember that the floppy disk is private and personal. It should be kept securely and removed from the computer after use.
- While using the disk additional, identification files are stored on your computer (the system cannot be accessed from any other computer).