TECHNICAL CONDITIONS OF INTERNET BANKING

Technical requirements for the use of the LHV Internet Bank

In order to take full advantage of the opportunities of the LHV Internet Bank, the user must be identified by his or her ID card, Mobile ID or PIN calculator.

ID cards function well:

- on Microsoft **Windows** operating systems (starting from Windows XP) with browsers Microsoft **Internet Explorer** (version 7 and higher) and **Mozilla Firefox** (version 3 and higher).

  Login and/or signing of payments may or may not be successful with other browsers.
- on Apple **Macintosh** operating systems (version 10.6.x and higher) with only **Firefox** (version 3 and higher).

  In case of Safari, you probably won't be able to enter into the LHV Internet Bank using your ID card.
- on **Linux** operating systems with **Firefox** (version 3 and higher).

  In case of Lynx, you cannot login to the LHV Internet Bank using your ID card.

For identifying the user and signing the payments with **Mobile ID** and a **PIN calculator**, you need to have **JavaScript** enabled in the browser you use.

Security in the LHV Internet Bank

Security is the factor of principal importance in developing the LHV Internet Bank. The Internet Bank users themselves and the hardware and software used by them also play an important part. Using of the Internet Bank is as secure as secure is the weakest link in the whole system.

1. The bank does the following for ensuring the security of the Internet Bank:

- Information between the Internet Bank user and the bank is encrypted (using the SSL3 or TLS1 method on HTTPS protocol).
- The Internet Bank user is identified by a unique identifier and the ID card, Mobile ID or PIN calculator.
- If the user attempts to log in for more than 5 times in vain, the PIN calculator will lock.
- The Internet Bank session will expire.

2. The client/user must do the following:

- To ascertain when opening the LHV Internet Bank that the correct address is on the browser address line (https://www.lhv.ee[1]) and that the connection is encrypted.
  The name of the certified person (AS LHV Pank [Ee]), name of the certification authority (Thawte) displayed in green on the browser address line and a closed padlock (which can also be on the lower edge of the browser window) are the evidence of authenticity and encryption.
- To keep his or her user ID and means of identification safely.
  Users of the LHV Internet Bank are identified only by entering their user ID's and PIN codes in the electronic environment of the Internet Bank. Representatives of LHV Bank never inquire for passwords or PIN codes. When somebody inquires for your user name or PIN codes by phone, e-mail or in another way, please refuse and inform the LHV Customer Support immediately thereof.
  Should you lose your ID card, you have to immediately inform the ID card help line 1777; should you lose your Mobile ID – the service provider having issued the SIM card; should you lose your PIN calculator – the LHV Customer Support.
- To set reasonable limits not in excess of his or her needs for the amounts of transactions that can be conducted within one day and one month.
- To protect the computer and its software used for logging into the Internet Bank (see also "In general about the Internet and security").
- After having finished using the Internet Bank, to log out of the Internet Bank – LOGOUT button in the header of the Internet Bank page.

3. Security elements

A user of the LHV Internet Bank is identified by means of security elements. The security elements issued by the Bank in compliance with the Bank's established procedure include the unique user name and a PIN

[1] or https://www.lhv.lv or https://www.lhv.lt

calculator, with the help of which the user can enter the Internet Bank. In addition to the PIN calculator, the user can also be identified using his or her Mobile ID or ID card.

If desired, it is possible to assign a temporary trading password and a temporary password for using the LHV forums. LHV does not recommend the use of passwords. Should you still wish to use temporary passwords, the password has to be as long as possible, contain many different characters and symbols, and should not contain any personal information that would be easy to guess. At the same time it should be easy enough to memorize the password so that there would be no need to write it down.

Should you have any doubts about that somebody else is using your account or you find problems relating to the security of the LHV Internet Bank, we kindly ask you to immediately call the Customer Support (+372 6 800 400).

In general about the Internet and security

Internet as a threat

Once the Internet was a closed network, which connected reliable computers and educated users. The logical bases for the functioning of this infrastructure were described in the 70's proceeding from trust and simplicity, and little attention was paid to security.

Today, in this same network, which has grown into a global one, operate inter alia cyber criminals, whose success depends on the efficiency of taking advantage of computers, including your computer, and efficient utilization of the information stolen (inter alia your credit card data, Internet Bank passwords, etc.). Operation of cyber criminals is facilitated by the fact that the logical bases of the Internet infrastructure are today basically just as insecure as some decades ago when the network had only reliable members and everybody trusted everybody.

Therefore, in order to avoid potential damages, it is reasonable for you as the Internet user to follow the principles that have been explained in detail but in simple language on this website.

Attacks independent of your habits

A computer connected to the Internet or LAN can be rather unprotected – even a freshly installed MS Windows operating system "listens" to the messages coming from the network and responds to them in case of need. Such service is for example the "*File and Printer Sharing*".

A capable criminal can deceive the alertness of the computer with a purposeful inquiry (so-called *remote exploit*) and achieve access to the documents of the owner of the computer, install malware or totally disable the computer.

How to protect yourself?

As a rule a properly adjusted firewall and functioning antivirus software helps against attacks. There are many companies which offer antivirus software but to those who use MS Windows we recommend to choose for example among these.

In addition to this you definitely have to install updates to your operating system, antivirus software as well as to all the software used in the computer.

Microsoft operating systems provide software updates automatically (unless the user has forbidden it). These can be installed manually from here.

Updates to the software used in your computer can be downloaded from the homepage of the software developer or by using the updating system of the software.

For example in case of Adobe Reader you have to choose *check updates* in the *help* menu.

You definitely have to keep Adobe Flash updated as errors in it are very frequently used in web-based attacks. You can check your available version here and download the most recent one here.

If you use for example LHV Trader, you certainly have also Java installed on your computer. Updates to it are offered by the Java software itself and you have to install them for sure.

In order to update **Mac OS X** you have to choose from time to time "Software Update..." from the menu with the picture of an apple and let the computer install the necessary updates.

In case of **Linux operating systems** the methods of installing updates depend on the distribution used. As a rule, the root user has to initiate the respective commands from the command line. E.g.,

- Ubuntu (4 commanda on one line, all required)
  aptitude update && aptitude safe-upgrade && aptitude dist-upgrade && aptitude safe-upgrade

- RedHat
  yum update
- Mandriva
  urpmi-update -a

Attacks taking advantage of your habits

Nowadays the attacks that take place with the (unknown) help of users (so-called *client side attack*) are the most dangerous and widespread. For example you are sent an e-mail to which a file with the extension .pdf, .doc, .jpg, .xlsx or another extension has been attached, which you are used to open and for the opening of which you have the required software.

As the contents of the e-mail received seem to be believable (e.g., you are invited to a seminar and the agenda is supposed to be in the .pdf document), you open the attached file using the Adobe Acrobat Reader, you examine its contents, you close the file, and you forget it in a few minutes.

But when the document was opened, the program launched a crafty code contained in it which installed a keystrokes logger and a hidden back-door in your machine through which the author of the attack takes control of your computer. Your antivirus software does not see any problem here as the software is unable to consider the method used for the attack as evil – this information reaches the antivirus software only in a few hours or in a worse case even in a few months.

Files containing evil code need not come by e-mail only. Attacks through MSN, Facebook, and other much-used communication channels are also widespread. In such cases your friend (seemingly) sends you a file and recommends opening it, or suggests that you visit a certain website using your browser. When you open the file the same happens that was described above, and when you open the website, a security hole in your browser is used for the attack.

As a rule, you as the user are unable to know about a well performed attack before money starts to disappear from your credit card or bank account.

How to protect yourself?

- Before opening any file you received by e-mail, please think whether its sender is credible and whether he or she has notified you in advance of sending this file.
- When you surf on the Internet, please think whether the page you are recommended to visit is reliable.
- If you find an apparently cool program, a screensaver or a new toolbar for your browser, please think whether you actually need it and whether it outweighs the possibility of losing the money in your bank account.
- If you have several computers at home, use only one of them for visiting your Internet Bank, making credit card payments and other such important things. With regard to that computer observe particularly carefully what you do with it – which websites you visit, which files you open, which software you install on it.

Your ID card, Mobile ID and PIN calculator

The ID card is relatively secure because even if the attacker monitors each of your keystrokes (and gets to know your PIN1 and PIN2), the attacker is still unable to get an access to your bank account because for authorisation a physical thing is needed – your ID card. But the attacker is unable to steal your ID card using the electronic channels.

The same applies to Mobile ID and PIN calculator but unlike in case of the ID card, the PIN calculator and the Mobile ID do not have to be connected to the computer.