Recommendations on computer security

trešdiena, 2018. gada 15. augustā 10:29

1. When working in online bank it is recommended to secure the computer or the mobile device with antivirus software.
In case the antivirus software is already installed, it is necessary to update it.

It is also recommended the installation of firewall programs and/or the other available hardware, such as – malware penetration prevention system, confidential information access control system confidential information access monitoring system etc. (IPS/IDS, DLP).

Firewall — a program for computer protection against attacks and unauthorized access from network.

IPS – software or hardware system for computer and network security, which detects **invasions or security violation and automatically protects** from them.
IDS – software or hardware feature intended for **detection** of unauthorized access to computer system or network or unauthorized management generally via Internet.
DLP - **technology for data leak prevention** outward data system as well as technical devices (software or hardware-software) for data leak prevention.
Useful sources:

- http://www.esidross.lv/ - security information portal
- http://windows.microsoft.com/lv-lv/windows/security-essentials-download — Microsoft anti-virus
- http://www.antivirus.lv/ - Kaspersky anti-virus
- https://www.avira.com — Avira anti-virus
- http://avg.com – AVG anti-virus
- https://www.virustotal.com — free on-line virus test
- http://secunia.com/ - computer-system audit
- http://www.zonealarm.com/ - firewall anti-virus
- www.zemana.com – anti-key-logger for protection from spyware
- www.malwarebytes.org — malware detection and removal program

2. Protection of the computer or mobile device by means of password. In case you need to leave the computer without supervision, it is necessary to use screen password protection. On computers with the Windows operating system, for screen lock they usually use the Win keys (the key with Windows logo, between Alt and Ctrl) + L.

3. It is necessary to update regularly the software — an operating system, the browser, the anti-virus software - on the device with which you work in online bank.

4. To limit access for the third parties to the device with which you work in online bank. It is not recommended to use publicly available devices — such as computers in an Internet cafe, hotels, and libraries. In case you are forced to use publicly available computer, then after work in online bank is completed, you have to log out by pressing the “Exit” button and close the web browser window.

5. Use division of computer user rights.

Division of computer user rights allows the admin user to allow/forbid use of computer programs and resources. For daily work it is not recommended to use the admin user profile as this user has full access to computer resources — installation of programs (also malware), removal of programs (also anti-virus programs), shutdown of programs (antiviruses, firewall), access to data of other computer users. For daily work, we recommend using the limited access rights — installation of programs is forbidden, possibility of shutdown of an antivirus is forbidden. In case it is necessary to install any program, it is possible to switch to the admin user profile.

Safe work in online bank

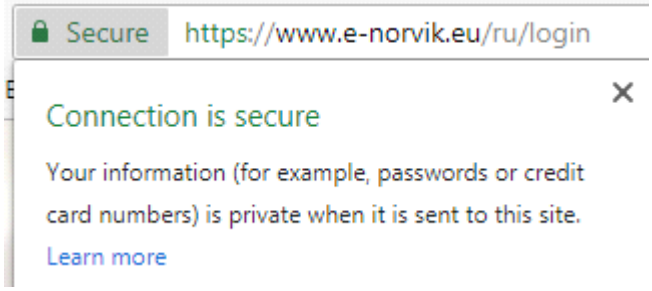
Safe work in online bank means mutual responsibility from both parties – *Norvik Banka* and online bank user.

To provide the highest level of safety is a mutual task

Please, rememmber that bank never requests data for authorization in online bank by e-mail, phone or any different way. Do not tell the password for your online bank, codes from identification tools to anybody. In case the third parties get access to your code card, security token or mobile device (authorization via SMS-pin) or you had suspicions that there is any security threat, please contact the bank security service immediately: (+371) 6704 1100.

Our recommendations for safe work in online bank:

1. While working in online bank, you must be convinced that the certificate of authenticity (SSL) is valid. The valid certificate in the part of https: address in address bar must be displayed in green color.



In addition, the name in the address bar must correspond to the address typed by you — www.e-norvik.eu.
In the certificate of authenticity in the field of *"Issued to:"* there has to be value www.e-norvik.eu, in the field of *"Issued by:"* there is specified value thawte Extended Validation SSL CA.
The certificate of authenticity (SSL) also provides the encoded connection between the client and online bank.

In case part of https: address is displayed in red color or there is a certificate SSL error mark in the browser, it means a possible threat to secure connection. In that case, please contact bank security service (+371) 6704 1100.

2. We recommend controlling history of bank payments and accounts balance regularly. You may use the possibility to check transactions in online bank via SMS.

3. You have to use complex passwords, containing from 8 to 16 symbols, to log in online bank. The password must contain small and big letters, figures, and special symbols. Do not use in the password easily guessed meanings, such as a full name, a machine number, nicknames of animals, the name of the cities, date of birth, registration number of the enterprise, etc. Do not write your password on a piece of paper or code card. When changing password do not use the previous one as the new one. In case you had suspicions that someone could steal your password, please contact bank security service (+371) 6704 1100, it is also necessary to change the password, it is desirable to carry out password change from other computer or device.

4. On completion of work in online bank, it is necessary to press the exit key and to close the browser. In case you had to use publicly available computer then it is necessary to clear cache and browser history, to remove files containing statement of the account or other files loaded from the online bank.

The main threats for online bank user

1. False letters, calls

   The most popular is “phishing” – mailing of false letters or making false calls on behalf of bank with a request to report authorization data. In addition, phishers try to obtain credit card information (card number, CCV2, PIN code, card expiration date) or client personal details. In false letters, phishers can duplicate corporate identity of bank.

2. False sites

   Rather often in false letters they use hyperlinks with the offer to authorize oneself in online bank or to receive additional information, these links will redirect the user on the false sites similar to the online bank site, the use of which helps the attackers to get access to user authorization data. There may be malware or spyware on the false sites.

3. False certificate of authenticity

   Attackers to disrupt encoded data link or redirect user to the false sites use false certificates of authenticity (SSL/https). In case the user agreed to use a not entrusted certificate, the attacker can not only pick up and decipher the data sent by user but also change these data. During the work in online bank, it is necessary to be convinced that the certificate of authenticity is the authentic one.

   In case of obtaining letters, calls with a request to report your online bank details, please report immediately about it to the bank security service (+371) 6704 1100.