These safety Rules and recommendations for working with Internet Banking System (hereinafter – System) were developed on the basis of experience of foreign banks and companies. These rules provide description of practical examples-schemes of intruders' actions aimed at obtaining unauthorized access to company accounts.

Take into account that the described below fraud cases did not take place in JSC «First Heartland Bank». The purpose of these Rules is warning our clients about all possible fraud situations over which the Bank has no direct control and at which the awareness and alertness of the clients is of crucial matter.

Please, note that the remote banking system has proven itself with the foreign companies as the most reliable and safe method of working with bank compared to information exchange by means of paper medium.

RULE №1. Under NO circumstances one should ever DISCLOSE ACCESS PASSWORDS to Internet Banking System.

Passwords represent confidential information and must be known only to a person for which bank has created login to access the System. System access password must have at least 8 digits, contain letters, numbers and special symbols.

It is prohibited to use auto fill and saving of passwords and user data in web browser (you have to cancel the suggestion by Internet Explorer to save the data at the computer used).

RULE №2. Under NO circumstances one should ever pass the DIGITAL SIGNATURE CERTIFICATE to any third party and should take all measures in order to prevent its unauthorized copying!

Digital signature certificate must be available only for the certificate owner and/ or to person authorized for certificate use according to the Legislation of the Republic of Kazakhstan.

In order to prevent copying of Digital Signature Certificate you must follow the following rules:

♣Use Digital Signature Certificate only at the moment of signing of payment documents in the System;

♣Do not keep Digital Signature Certificate in public places;

♣Do not pass Digital Signature Certificate to any third parties;

♣It is strictly prohibited to use Digital Signature Certificates in publicly accessible computers (for example, in internet

cafes).

Possible actions schemes of intruders aiming to obtain login and password to Internet Banking System, Digital Signature Certificate:

Option 1

Presenting himself as Bank employee, intruder calls to company employee having an access to Internet Banking System and by referring to technical error in the system or to any other reason asks the employee to name his login and password to access the Internet Banking System.

What you must pay your attention to:

A) A Bank employee would never request you to provide your password for System access. In order to solve technical or other issues in the System Bank employee does not need to know your personal password.
B)Whether you know this Bank employee, whether his voice sounds familiar to you.

C)If you have call recognition option on your phone – write the number appearing on your phone when Bank employee calls you.

Which actions you must take:

A)Under no circumstances you must tell your password for System access;

B)Try to remember or write the name of employee calling, his phone number;

C)Immediately call the Bank by the following numbers: Almaty (727) 2581505 and notify about such case.

Option 2

To your electronic mailbox you receive a message from Bank employee, System administrator of authorized body representative. Under some excuse the sender asks you to send your login and password for System access in respond to this letter. In this case the e-mail address of a sender may look as a true one, belonging to Bank, for example, administrator@fhb.kz (might be compromised).

What you must pay your attention to:

A) Bank employee would never request you to provide your password for System access. In order to solve technical or other issues in the System Bank employee does not need to know your personal password.
B)Whether you know this Bank employee the name of which is provided in the end of letter; are there any contact details of this Bank employee.
C)Which address is shown in the “To” field if you press “Reply” button (when replying to message the real e-mail address may be shown in the corresponding field).

Which actions you must take:

A)Under no circumstances you must share your password for System access;

B)Try to remember or write the name of employee calling, his phone number;

C)Immediately call the Bank by the following numbers: Almaty (727) 2581505 and notify about such case.

RULE №3. Enter and use Internet Banking System only through https://online.fhb.kz/ or https://online1.fhb.kz/ website

When using the System pay attention to website address indicated in your web browser address bar. In case you notice that the website address in address bar has changed, do not enter your login and password, immediately close this website and call the Bank.

In case if the Bank has actually changed the web address of Internet Banking system, you will certainly receive an official letter from Bank stating the change of address and also this information will be placed at the main Bank website http://fhb.kz/

Possible fraud schemes with phishing website

Option 3

You receive a notice by phone or by e-mail on change of Bank's website address through which you enter Internet Banking System. In this case the e-mail address of a sender may look as a true one, belonging to Bank, for example, administrator@fhb.kz (might be compromised).

What you must pay your attention to:

A) Whether you know this Bank employee, whether his voice sounds familiar to you (if there was a call).

B)If you have a call recognition on your phone – write the number appearing on your phone when Bank employee calls you (if there was a call).
C)Whether there are any contact details of this Bank employee (if the notice was sent by e-mail).

D)Which address is shown in the "To" field if you press "Reply" button (when replying to message the real e-mail address may be shown in the corresponding field).

Which actions you must take:

A) Unless an official notice/ confirmation received from the Bank regarding the change of System website address under no circumstances you should visit the website indicated by unknown persons or enter your login and password for Internet Banking System access at the unknown website.
B)When receiving the notice from Bank on change of Internet Banking system website address you have to contact the Bank and confirm the information received.
C)In case of such situations or in case of any doubts regarding the site authenticity immediately contact the Bank by the following numbers: in Almaty (727) 2581505 and notify about such case.

Option 4

When entering the Internet Banking System website https://online.fhb.kz/ or https://online1.fhb.kz/ the website address automatically changes to another one. In this case a warning on website certificate mismatch may appear on your computer.

What you must pay your attention to:

A) When using the System pay your attention to website address indicated in your web browser address bar.

B) When using the System pay your attention to any discrepancies in the processing or order of entering the System (compared to how the System worked before).

Which actions you must take:

A) Do not enter your login and password for System access in case you have any doubts about its authenticity.

B)Immediately close this website.

C)Immediately contact the Bank by the following numbers: in Almaty (727) 2581505 and notify about such case.

RULE №4. In case if your password for Internet Banking System was compromised, your Digital signature certificate was stolen/ lost or illegally copied, you suspect the unauthorized use of System and or Digital signature certificate and in other cases that may lead to unauthorized access to your company accounts, you must immediately notify the Bank on this by the following numbers: in Almaty (727) 2581505.

RULE №5. Do not store at your computer and do not install files or programs received in electronic messages from unknown persons.

Files received from intruders may contain viruses or programs aimed at obtaining your logins and access passwords, obtaining Digital Signature Certificates.

Possible intruders' action schemes aimed at obtaining login and password for Internet Banking System access,

Digital Signature Certificate

Option 5

To your e-mail you receive a message with attached file from the unknown person who may represent himself as a Bank employee. Referring to the update of Internet Banking System, asking for assistance in solving technical issues or using other reasons he asks you to save or install the attached file or program. In this case the e-mail address of a sender may look as a true one, belonging to Bank, for example, administrator@fhb.kz (might be compromised).

What you must pay your attention to:

A) Whether you know this Bank employee the name of which is provided in the end of letter; are there any contact details of this Bank employee.
B) Which address is shown in the "To" field if you press "Reply" button (when replying to message the real e-mail address may be shown in the corresponding field).

Which actions you must take:

A) Do not save or install files and programs received from unknown persons including suspicious Bank employees.

B) contact the Bank by the following numbers: in Almaty (727) 2581505, notify about such case and confirm the fact that this message was really sent by the Bank employee.

The described above fraud schemes and intruders' action schemes are not exhaustive. Bank will apply all measures for timely distribution of information on new fraudulent contrivances of intruders. Nevertheless, you must pay attention to all suspicious situations, be alerted and in case of similar situations immediately contact the Bank by the following numbers: in Almaty (727) 2581505.