TENGRI BANK

GUIDE TO INFORMATION SECURITY DURING WORK WITH REMOTE BANKING SERVICE OF "TENGRI BANK" JSC

2016

Dear customers of Tengri Bank!

Over the last years, there has been a significant increase of fraud attempts in cyberspace aimed at customers of financial organizations, and fraudulent schemes are becoming more sophisticated.

It is necessary to clearly understand that in the remote interaction between the Client and the Bank, security depends entirely on the efforts of both parties and must be provided by mutual assistance. The most sophisticated means of defense can be powerless if you neglect elementary security measures.

At the same time, as a rule, fraudsters do not direct their efforts to attack the bank's protected systems, but try to influence the client in the expectation that the level of protection on the client's side will be significantly lower or the protective measures on the part of the client will be completely absent.

Tengri Bank has prepared this guide to help our customers to do as follows:

- To better understand actual treats and risks that may be caused to customer during use of remote banking services;
- To be able to identify typical strategy of unauthorized obtaining of confidential information by fraudsters;
- To identify situations and cases of high risk;
- To ensure required level of security and comfort during use of system RBS.

WE HIGHLY RECOMMEND YOU TO READ THIS GUIDE AND CONSISTENTLY FOLLOW OUT INSTRUCTIONS DURING WORK WITH RBS.

1. TYPICAL METHODS OF FRAUDSTERS IN FRAUDULENT SCHEMSA IN SYSTEMS OF REMOTE BANKING SERVICES (RBS) AND THEIR MAIN CHARACTERISTICS

Actions of fraudsters are aimed to possessing confidential information of customer – for example, passwords, code phrases, personal keys, etc. If they succeed, fraudsters plan to further use received information, also for attempts to send Bank requests on behalf of customer.

In order to achieve this fraudsters try to use different methods and channels to affect customer and their combination.

Email messages

Fraudsters often use fake emails in their schemes. The easiest method is bulk messaging as advertising messages (so called spam). The danger lies in the fact that when you go to link placed in such message, there is a risk to be transferred to web-site which main goal is to spread computer viruses and other types of malware. In case of computer infection, viruses can seamlessly for user to collect, capture and send fraudsters confidential information, for example - passwords.

More sophisticated and dangerous type of malicious use of email is Bank messages imitation. Tying to make messages look more real, fraudsters may use corporate logos, faking email address of sender, etc.

In this case, fraudsters aim at various pretexts to lure the client to a fake web site that mimics the present site of the Bank and encourage the client to take actions that will lead to the disclosure of confidential information, for example, to enter your password for logging into the RBS, your mobile phone number, etc.

More differential characteristics that is evidence of the fact that email message is fake as follows:

- Message content evoke You to take immediate actions, which can also be emphasized by the possibility of the onset of negative events otherwise. Prepositions can be various - possible account blocking, detection of an unauthorized operation on your account, the need to establish an "urgent update", confirm in the system your data in connection with "system recovery after a failure" and the like;
- In message there is web-site link,supposedly leads to Bank system site, which are requested to be login into RBS. If customer tries to go to such link, it may be at fake site, that imitates real Bank web-site, or may be occur a pop-up window in which customer may be asked to enter or “confirm” his/her confidential information for login into system;
- In subject and/or body of message there may be mistypes, wrong spelling of words, merging or broken words. Such tricks may be used by fraudster in order to override automatic systems of identifying and countering spam.

Real email messages from «Tengri Bank» JSC do not request You to:

- Go to link in RBS and do not request You to login into system by link in email;
- Notify, update or confirm Your confidential information, including passwords for login into RBS, code phrases, mobile phone number or his model, ect.

SMS-messages

Like email messages, fraudsters may try to evoke customer to take actions of disclosure of confidential information of customer by sending him/her fake sms messages: Such SMS messages can closely simulate authentic Bank messages, but the following characteristics will help you distinguish between fake messages in case they are received:

- Content of message evokes You to take immediate actions
- In SMS-message there is a request to install additional software, «security softwareи», etc to Your smartphone and there is a web-site link for taking such action. Going to such link can lead to infection of your smartphone with a specially designed virus, which can then suppress the display

of authentic SMS messages from the Bank, and confidential information sent by the Bank in SMS messages (for example, passwords for operations) will be secretly transferred to intruders;
- Web-site link for login into RBS and request to login into system;
- SMS-message was sent from unknown telephone number, not from official number of Bank.

If received SMS-message alert You or made You doubt or you received an SMS with notification of the transaction or a request to confirm an operation that you did not conduct, immediately contact the Bank using the official contact numbers specified in your client documentation.

Fake web-sites

Another trick which is often used by fraudsters is so called phishing – creating fake web-sites that are maximum similar in design to authentic web-site of financial organizations.

Then fraudsters, sending fake e-mail messages to the client, SMS messages, try to lure customers to a fake Web site and perform an "entry" into the system, thereby revealing their passwords and other confidential information to attackers. Also dangerous are computer viruses that, in the event of infection of the client's computer, can track attempts to enter remote banking systems and redirect them to spoofed sites.

Alternatively, instead of switching to a fake site, malicious software can open additional or pop-up windows in a web browser program in which the client's confidential information can be requested, allegedly on behalf of the Bank.

You can identify fake web-site by following characteristics:

- Web-site address may be totally different from official web-site of RBS; Wherein, difference in address may be minimum, for example only one or few symbols, because creating fake site, fraudsters try copy authentic site at maximum;
- Web-site link was received by You through email or SMS messages;
- When you log on to the site, your web browser informs you that the authenticity of the site can not be confirmed, a secure https connection is not established, or there are problems with the SSL certificate of the website;
- When log into site besides Your Login and Password, You are also required to provide some additional information and/or personal data, for example to «confirm» mobile phone number, specify manufacturer of model of Your mobile phone or install «update» or additional software.

If You received message that contain web-site link and request to log into RBS, or You have doubts that You are at fake web-site, then immediately leave site and notify Bank about it by contacting official phone number specified in Your customer documentation.

Infecting computer by malicious software:

Often, cybercriminals try to infect a user's computer with malicious software, such as computer viruses, spyware, keystroke interceptors,

Fraudsters try to place malicious software on various websites - from sites with dubious content and to social networking sites and news sites with insufficient protection.

Infecting a user's computer can occur unnoticed when a user visits these sites, and starting point is often e-mail with web links sent to the user as an address or as part of a mass spam mailing.

Be extremely wary of e-mail messages received from unknown senders, especially if such messages contain attached files or web links. Very often, web links in such messages can lead you to a site from which attempts will be made to infect your computer.

The use of modern anti-virus software, its timely update and regular full checks of your computer for viruses are adequate measures to reduce the risk of infection and / or prompt detection of malicious software.

Reasonable caution when visiting websites will also help you reduce this risk.

Telecomunication

Fraudsters may try to use telephone communication in combination with "social engineering" methods to gain access to your confidential information.

Remember that real employees of the Bank will never ask you to provide your passwords for entry and other confidential information by phone. Contact information (phone numbers and e-mail addresses) can be changed by the client only by personal application to the Bank.

Only if you yourself called the Bank, depending on the type of treatment, the employees of the bank identifying you may ask to name your personal code phrase for purpose of confirming your identity.

Keep your secret code secret and do not share it with anyone.

If you received an incoming call on behalf of Bank, and it arouses your suspicions, then do not rush to answer caller's questions. Specify purpose of call, name, surname, position and department of caller and on what phone you can contact. Then, call Bank back to contact numbers listed in your client documentation in order to verify authenticity of received call.

The Bank also reports that it does not use automatic information systems in its work to make calls to its customers. If you received an incoming call on behalf of Bank and automatic notification system asks you to enter your password or other confidential information in tone mode, this is a clear indication of fraudulent activity. In this case, contact Bank immediately.

2. PERSONAL SECURITY MEASURES AND RECOMMENDATIONS FOR USE OF REMOTE BANKING SERVICES

1. Install and use modern antivirus software, personal network-level firewall (brandmauer, firewall). Ensure daily update of your antivirus bases.
   The Best solution 1) switch on automatic update of Your antivirus software and 2)regularly perform complete scanning of You computer.

2. Modern smartphones and tablets are computing devices, comparable in complexity and capabilities with long-established personal computers. Install modern anti-virus software on your smartphone or other device that you use to interact with RBS.

3. Always install security updates for the operating system and key applications (such as a web browser) produced by manufacturers in time.
   The best solution – switch on automatic update.

4. Avoid permanently working on your computer under an account with administrative authority (for example - Administrator). Performing daily work, including the use of Internet resources, under an account with broad authority makes your computer much more vulnerable to infection with viruses, spyware and other malicious software.

   The best solution - to perform ordinary tasks, use an account with limited access rights. Use the administrative level of access only for those tasks where it really is required.

5. Avoid working with other websites during a session using the RBS.

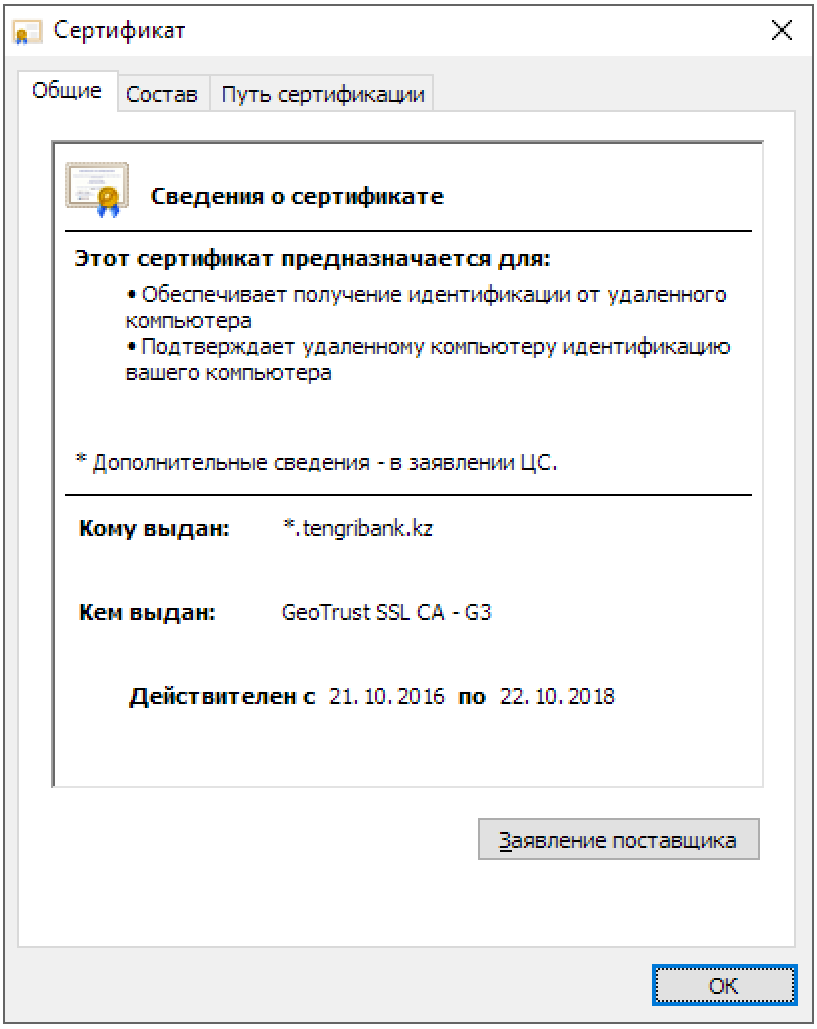
   Best practice: Close all browser windows before you start working with the RBS. Then open web browser application and log in to RBS.
6. Always log in to RBS from official web-site
   Never log in to RBS by link received by email message (e-mail) or SMS-message.

   Fraudsters often use email messages, imitating messages from Bank, in order to lure user to fake web-site. Opposite, Bank never posts links of RBS access in outgoing email letters addressed to customers.

   The best solution: spend a few extra seconds and type the RBM system address manually in the address bar of the web browser.

7. Before entering your login and password for logging in to the RBS system, be sure that

a) A secure connection session (https) is established with the website.
б) You are on the original site of the RBS system, and the current SSL certificate is issued by Tengri Bank.



Сведения о сертификате

Этот сертификат предназначается для:

- Обеспечивает получение идентификации от удаленного компьютера
- Подтверждает удаленному компьютеру идентификацию вашего компьютера

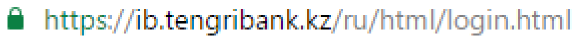
* Дополнительные сведения - в заявлении ЦС.

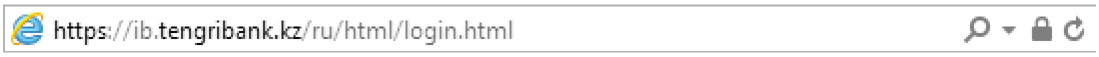
Кому выдан: *.tengribank.kz

Кем выдан: GeoTrust SSL CA - G3

Действителен с 21. 10. 2016 **по** 22. 10. 2018

To display the SSL certificate data, click on the image of the secure connection (private lock) in the web browser. It may look different (depending on the web browser).


https://ib.tengribank.kz/ru/html/login.html


https://ib.tengribank.kz/ru/html/login.html

8. After log in system always pay attention to information on last log in system. This information is available at main page of account and reflects date, time and network address, from which the last log in system under Your profile was made.

If you have a suspicion based on this information that someone else was logged in under your account - immediately change your password and contact the Bank by contacting the numbers listed in your client documentation.

9. Use strong passwords to log in RBS and regularly change them.

Strong password shall be as follows:

- Shall be at least 8 characters long. Longer passwords are more reliable. With each additional symbol, the stability of the password for selection is significantly increased;

- The password must include uppercase and lowercase letters, numbers and special characters;
- Do not select repetitive sequences of characters or keystrokes located in easily anticipated order on the keyboard (for example, Qwerty123! Is a very vulnerable password, despite its length and apparent complexity);
- Do not use as passwords the names, dates of birthdays of people close to you and other personal information that, if desired, attackers can still easily find out from open sources;
- Password has to be changed regularly – not less than once every 90 days;
- A strong password should be easy for you to remember and not require a record. Once a strong password is recorded, it does not matter - on paper or in electronic form, it ceases to be reliable.

10. Do not use your password to RBS as password for any other systems. Especially – to systems, located in Internet (for example, email, social networks, Internet shops, etc.). Requirements to level of security and safety of such systems may be lower, and possible hack into such system, You may not even know about, may cause risk of disclosure of Your password.

11. Never tell password to key file to anyone, recorded in USB e-Token, used for work in RBS;

12. After performing operations in the RBS system, or during a long absence in the workplace, physically remove the USB eToken and store it in a secure place inaccessible to unauthorized persons, before the following operations.

13. Ensure confidentiality of Your password, code phrase, personal USB eToken data storages. Do not tell any one Your password on any conditions. If You have doubts that Your password has become known to anyone else other than You – immediately change Your password by using function «Change password».

14. When log in RBS take into account, that in order to ensure confidentiality of Your password and its safety in case of its attach by fraudsters, after a number of unsuccessful login attempts with an incorrect password, your access to the RBS system may be temporarily limited or blocked.

15. Always correctly finish working session in RBS using pictogram of system «Log out» in top right corner of system display. Then close web-browser.

16. Bank strongly do not recommend to access RBS using guest working places (for example internet booth) and/or public wireless access networks (Wi-Fi), for example in cafes, restaurants, airports, hotels, office centers, etc. because these conditions and methods of RBS usage are cases of increased risk of interception of confidential information. If You still had to use RBS in these conditions, change Your passwords as soon as possible, using as access environment with a higher level of trust.