Recommendations for Safe Work with the Electronic Banking System on the Internet

JSC “ProCredit Bank” strives to ensure transparency of client transactions and confidentiality of information in its activities. When offering services to our clients, we are constantly working to improve the quality of our service, reliability and safety of the Electronic Banking System.

However, the Internet and e-mail can be used by fraudsters to obtain confidential information for further fraudulent use, and therefore we recommend that you always observe a few simple rules aimed to ensure safe work with the Electronic Banking System.

Basic precautions:

Log in to the Electronic Banking System of JSC “ProCredit Bank”

To log in to the Electronic Banking webpage of JSC “ProCredit Bank”, use only the address https://probanking.procreditbank.com.ua entered MANUALLY in the address bar of your browser or use your own bookmarks. Do not respond to e-mails with requests to send your personal or financial information and do not follow the links provided, as all e-mails with requests for confidential information are fraudulent. If you have any questions, call the Contact Centre of JSC “ProCredit Bank” by phone numbers 044 590 10 00 or 0 800 50 09 90 (all landline calls in Ukraine are free).

Secure password storage:

Never share your login, password or other confidential information with any third parties. JSC “ProCredit Bank” and officers of law enforcement agencies never send requests for confidential information from client via e-mail, never send letters with requests to provide confidential information, login or password, and never send software to be installed on your computers by e-mail.

Money security:

Do not pay attention to “sincere” e-mails describing methods of making money on the Internet. Attractive offers of easy money are frauds aimed at obtaining confidential information about your accounts.

Computer for working with the Electronic Banking System:

Use licensed copies of operating system and software on computers used to work with the Electronic Banking System. Use specialized security software at your workplace: personal firewalls, antispyware and anti-virus software, etc. with the maximum possible security settings. Avoid using the Electronic Banking System from computers in public places (Internet cafes, libraries and Free Wi-Fi zones), as well as from other computers the settings of which you cannot control.

Additional precautions:

1. Be sure to remember your password and other confidential information **by heart**. We recommend that you delete all messages containing personal information, such as passwords. We recommend that you disable the autocomplete feature.

2. Do not use the same passwords for the Electronic Banking System and for other programs.

3. When you change your password, the new password must consist of at least 8 characters and include a set of lowercase and uppercase letters, numbers and special characters.

4. Never share your login, password or other confidential information with any third parties (including your family members and friends).

5. JSC "ProCredit Bank" never requests passwords of clients who call the Contact Centre.

6. Always use the "Login" link on our website to access the Internet Banking System in your browser, and always log out of the Internet Banking System by clicking the "Log out" button.

7. After you have logged in to the Electronic Banking System, do not leave your computer unattended.

8. Restrict access to computers used for work with the Electronic Banking System for the staff not involved in working with it.

9. Depending on your Internet browser, the status bar may be partially or completely green. By clicking on the lock symbol, you can check which authority has issued the certificate. If the lock is open or if the certificate has not been issued by **JSC "ProCredit Bank"**, do not perform any operations and contact the bank immediately.

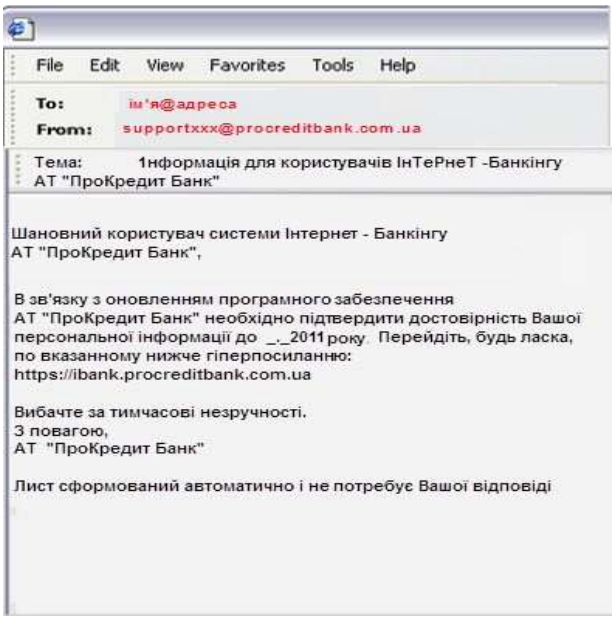
10. **If you notice suspicious changes in the work or interface of the Electronic Banking System of JSC "ProCredit Bank", please call** the Contact Centre of the bank by phone numbers 044 590 10 00 or 0 800 50 09 90 (*all landline calls in Ukraine are free)* or send us an e-mail to ukr.cc@procredit-group.com

Recommendations for protection against fishing

What is fishing?

Fishing is a type of Internet fraud, which aims at gaining access to confidential information of users, namely logins and passwords.

This is made through mass e-mail or message campaigns in social media allegedly in the name of well-known organizations, such as banks. Such letters usually contain a direct link to a website that does not look different from the real one. After users go to a fake page, fraudsters try various psychological tricks to force them to share their login and password used to access a particular website. After fraudsters obtain users' confidential information they can use users' personal accounts and bank accounts for their own purposes.


File Edit View Favorites Tools Help

To: ім'я@адреса

From: supportxxx@procreditbank.com.ua

Тема: 1нформація для користувачів ІнТеРнеТ -Банкінгу АТ "ПроКредит Банк"

Шановний користувач системи Інтернет - Банкінгу
АТ "ПроКредит Банк",

В зв'язку з оновленням програмного забезпечення АТ "ПроКредит Банк" необхідно підтвердити достовірність Вашої персональної інформації до _._2011 року. Перейдіть, будь ласка, по вказанному нижче гіперпосиланню:
https://ibank.procreditbank.com.ua

Вибачте за тимчасові незручності.
З повагою,
АТ "ПроКредит Банк"

Лист сформований автоматично і не потребує Вашої відповіді

Example of a fishing letter

Signs of fishing e-mails:

1. Sender's address

The e-mail address displayed in the field

"From:" It is NOT a guarantee that the e-mail was sent through the e-mail system of JSC "ProCredit Bank".

Fishing e-mails usually have the form of an e-mail, which does not look different from the original sent from the e-mail system of JSC "ProCredit Bank". In most cases, criminals do not know your name and therefore will use an anonymous form of addressing you, such as "Dear Customer".

2. Emergency nature of the message

In order to increase the number of responses, fraudsters try to give the message an emergency nature outlining the time limit, and cause the user to take unconsidered actions.

3. Errors in the subject of the letter

As a rule, the "Subject" field in fishing e-mails contains different letter cases, a set of letters and numbers, grammatical or typographical errors (for example, eRrOr, 1nformat1on) to avoid filters of e-mail programs.

Part of the ProCredit Group

ProCredit Bank ПроКредит Банк

Recommendations for protection against farming

What is farming?

Farming means the practice of replacing the IP address of the home page with a fraudulent IP address. The user is automatically redirected to a fake website without even knowing it.

How to recognize a fake website?

1. **Website address**

Example of the address bar

Most farming methods involve creating an impression that fake links to farming websites are links of real organizations. Fraudsters often use mistyped addresses or subdomains.

In fact, a website address (URL) consists of a set of numbers and letters, and the content of the website is fake. But some of the information and uncritical links may be original.

2. **Pop-ups**

Using various malicious software, fraudsters can create and place fake pop-ups requesting confidential information based on a legitimate website. In this case, the real website of the bank will be displayed in the background. This way, all the information you enter in the fake pop-up will be available to fraudsters.

How to protect yourself from fishing and farming attacks?

JSC "ProCredit Bank" never sends requests for confidential information from client via e-mail, never sends letters with requests to send confidential information, login or password, and never sends software to be installed on your computers by e-mail.

Observance of the rules below will allow you to successfully resist fraud attacks:

1. Never share your login, password or other confidential information with any third parties. Do not respond to e-mails with requests to send your personal or financial information and do not follow the links provided, as all e-mails with requests for confidential information are fraudulent.

2. If you have received a dubious e-mail on behalf of JSC "ProCredit Bank", please inform the Contact Centre of the bank by phone numbers 044 590 10 00 or 0 800 50 09 90 (all landline calls in Ukraine are free), or forward the dubious e-mail with your comments to the e-mail address: ukr.cc@procredit-group.com

3. Use the latest browser version. Browsers such as Internet Explorer, FireFox, Google Chrome, Opera are regularly updated and have a fishing protection filter.

4. When transmitting personal information always check and use an encrypted connection. When using a secure connection, a website address always starts with "https://", and not with http://. Also, make sure that the domain name in the URL of the loaded page is spelled correctly and that you are not redirected to a domain name with a slightly different spelling, possibly with additional letters or letters with different positions. Immediately terminate the session if they are invalid or your browser shows an error message.

5. When disclosing confidential information, make sure you are on an encrypted home page (as indicated by the lock symbol in the status bar). Clicking the lock symbol, you will be able to view the security certificate of the page. The domain name indicated in the certificate must match the name of the home page you have just accessed.

6. Call the Contact Centre of JSC “ProCredit Bank” by phone numbers 044 590 10 00 or 0 800 50 09 90 (all landline calls from in Ukraine are free) or send us an e-mail to ukr.cc@procredit-group.com, when the situation seems suspicious to you.