

SECURITY RULES

Financial frauds and deceptions are becoming more and more complex. Hence, to provide high quality services and protect you from information threats we provide you with information that will help you to be more secure and protected.

AEB Mobile and AEB Online Banking

Secure access to AEB MOBILE application

AEB Mobile system is designed for ARMECONOMBANK OJSC (hereinafter: the Bank) customers to enable making transactions through the app. The customers using the system may manage the bank accounts 24/7 at any time from elsewhere without visiting the bank.

1) The real appearance of the downloaded application is as follows:



Picture 1

The false versions often include sections to add additional pictures or fill in data.

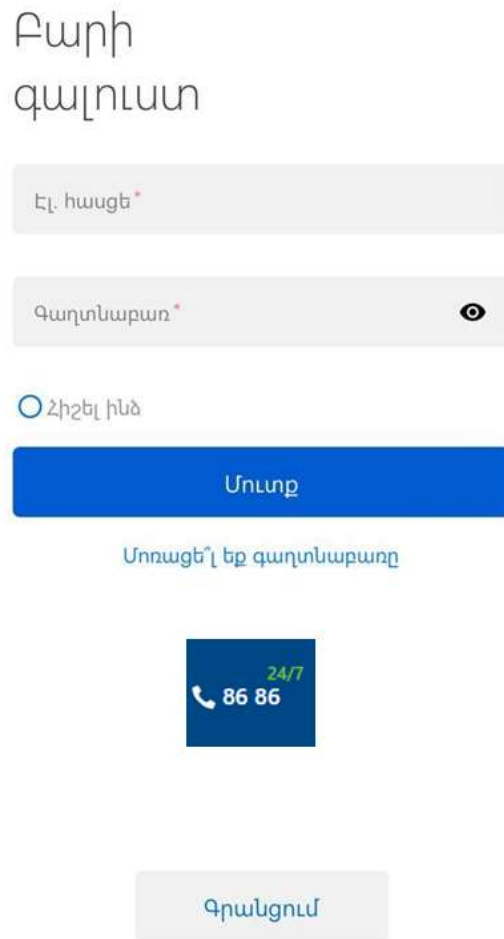
Some organizations and entities introducing themselves as intermediary lending companies or agents by the bank mislead the citizens, offering various services, including opening bank accounts in any of the branches of the Bank, accepting payments for services and making your login/password of Mobile Banking available to them, etc.

- 2) Do not collect your application password to access a suspicious application that differs from the real one.



The image shows the login page of the real application. It features the title "Բարի գալուստ" (Welcome) at the top. Below the title are two input fields: "Էլ. հասցե*" (Email address) and "Գաղտնաբառ*" (Password), both with red asterisks indicating required fields. There is a small eye icon to the right of the password field. Below the input fields is a radio button labeled "Հիշել ինձ" (Remember me). At the bottom, there is a blue button labeled "Մուտք" (Login) and a link "Մոռացել էք գաղտնաբառը" (Forgot your password?) below it.

Picture 2. Real application login page

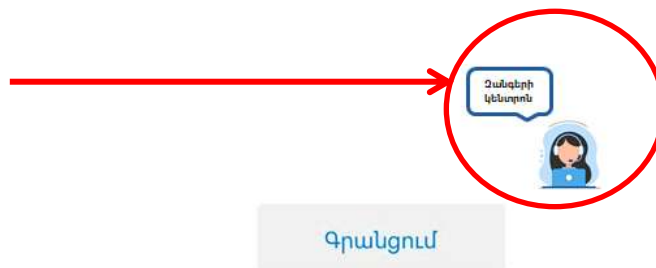


The image shows the login page of a false application. It features the title "Բարի գալուստ" (Welcome) at the top. Below the title are two input fields: "Էլ. հասցե*" (Email address) and "Գաղտնաբառ*" (Password), both with red asterisks indicating required fields. There is a small eye icon to the right of the password field. Below the input fields is a radio button labeled "Հիշել ինձ" (Remember me). At the bottom, there is a blue button labeled "Մուտք" (Login) and a link "Մոռացել էք գաղտնաբառը" (Forgot your password?) below it. Additionally, there is a dark blue square button with a white telephone icon, the number "86 86", and "24/7" in green text. At the very bottom, there is a grey button labeled "Գրանցում" (Registration).

Picture 3. False application login page

Բարի գալուստ

 Հիշել ինձ

Մոռացե՛լ եք գաղտնաբառը

Picture 4. False version which includes redundant images

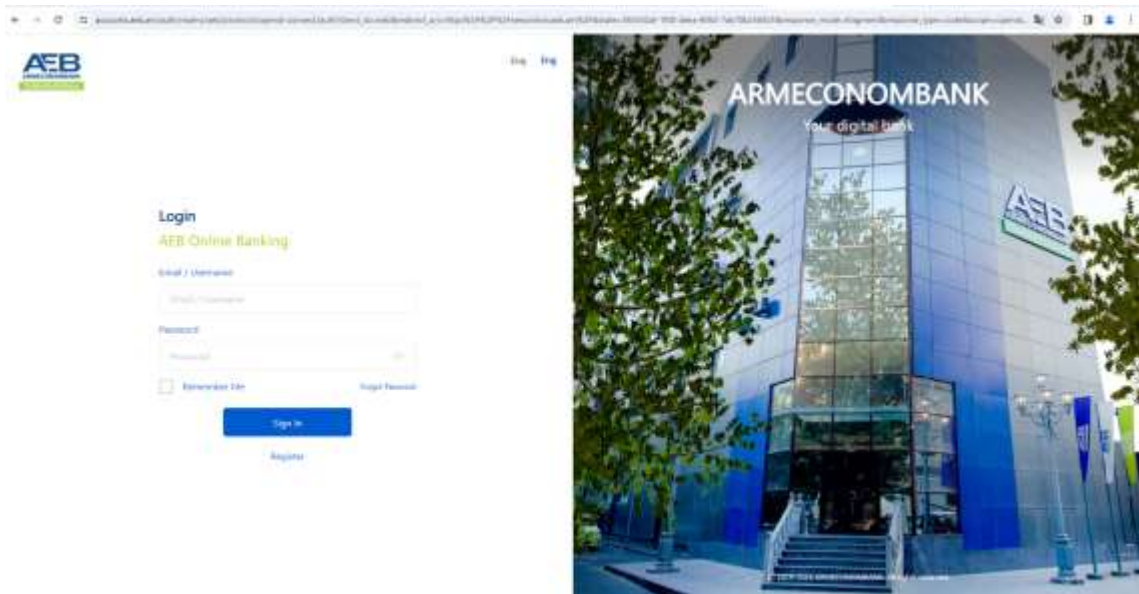
Secure access to AEB Online application

AEB Online Banking system is designed to enable the customers of ARMECONOMBANK OJSC (hereinafter – the Bank) to execute transactions via the Internet. The users of the system (LE, PE, PE clients) can manage their bank accounts 24/7 without visiting the bank at any time, from elsewhere.

To join the AEB Online Banking system an Internet browser and Internet connection is needed.

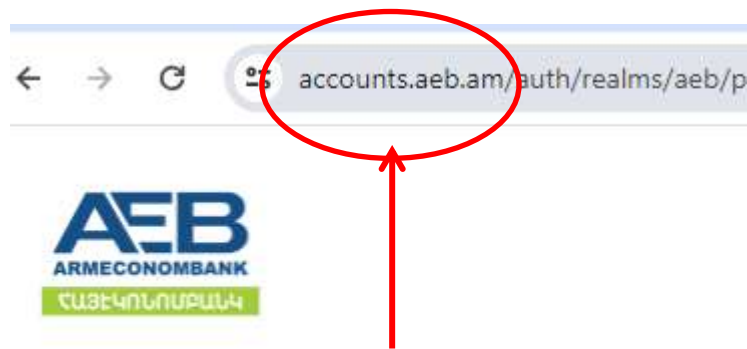
LOGIN TO SYSTEM

In case you are a PE client of the bank and a system user, go to <https://newonline.aeb.am> link on Internet browser or Bank's website (<https://www.aeb.am/>), select AEB Online service after logging in, afterwards fill in your e-mail address (your login) which you have submitted to the bank for registration, then the Password /a temporary password which the User must change after receiving from the bank in accordance with the required format/ and click Enter button (Picture 5).



Picture 5

It is strongly recommended to pay attention to the link, it should start like this:



Do not login to AEB Online Banking from links on other websites.

If, in order to make a payment on any commercial website, you are asked to go through the attached links or click on the attached AEB logo, with which you will supposedly be able to access the AEB Online Banking platform more easily and quickly, then do not go through those links and do not enter a login/password.

ATTENTION

To avoid potential frauds:

- Do not post your card details on suspicious details. The links in social networks automatically lead you to a place, where you can provide them with your full personal data with one tap/click. Use websites starting with https:// note, as the last s letter is the website security guaranty. Verify, then trust.
- Do not provide your personal (name, surname, date of birth, year and/or address) or financial (credit/debit card data (including the PIN)). If the caller introduces himself/herself as a bank employee, verify with him the account information.
- Never reply to suspicious SMS messages. Verify the phone number the message has been sent. If it from the Bank, contact the round-the-clock 86-86 phone number and clarify the issues that concern you.
- Avoid providing your personal data to unknown parties or companies neither by phone call, letter or e-mail nor by social media.
- Avoid the use of services provided by intermediaries or individuals, do not provide your personal data, identity documents, the mobile app data to third entities and organizations to fill in credit applications or acquiring banking services instead of you applying romte communication means.

ATTENTION

ARMECONOMBANK OJSC will never contact you:

- To request a PIN code or password of the card,
- asking for a three-digit security code (CVC) on the back of the card,
- asking for one-time verification codes received through an SMS or e-mail,
- asking for a password of Mobile Banking app,
- for transferring the the amount of the account to another account for security reasons.