Part of the ProCredit Group

ProCredit Bank

How to use e-banking/m-banking safely?

ProCredit Banka ProCredit is committed to offering you the required security in your online banking transactions and protect your account data. In fulfilling this commitment, ProCredit Bank uses the top-notch security software and implements a multitude of security processes.
Nevertheless, you must know that Internet and e-mails may be used as tool for illegal purposes and activities. For this reason, we always advise you to take some simple measures that ensure security in your various bank transactions.

Tips to be stay safe online

› Know who you are dealing with

Always access e-banking by pressing the bank link https://ebanking.procreditbank.com.al in your browser, or use m-banking by accessing the official application.
Do not access e-banking/m-banking by using a link sent to you via e-mail and never insert your personal data in that link. For any information that feels suspicious, please do contact our Contact Centre +355 4 2 389 389.

› Save your password in a safe location

Always be careful with e-mails and phone calls where you are required to disclose personal information, for example the number of your debit/credit card. ProCredit Bank or Police shall never contact you to give information on your password. Keep this data secret. Take care not to share this information to any person, particularly if you do not know the person in question.

› Keep your electronic devices safe

Always use antivirus updated to the latest version and install a personal firewall. The browser you use to navigate on the internet must be latest version and contain all the security updates. Above all, take extra care when you use internet from Internet Cafés, in public premises or when you are not using your computer /phone.

› Careful with your money

Do not be cheated by apparently sincere e-mails that offer you easy money. If you find it “too good to be true”, it most probably is a hoax. Pay particular attention to e-mails you receive from abroad, because such e-mails are very difficult to authenticate whether the sender is the one, he/she claims to be.[1].

For further information, please refer to the official website of cyber security specialists: http://www.staysafeonline.org/stay-safe-online

1) Please refer to document “How to protect ourselves from phishing?” published on the e-banking section of the Bank’s website.

Additional measures

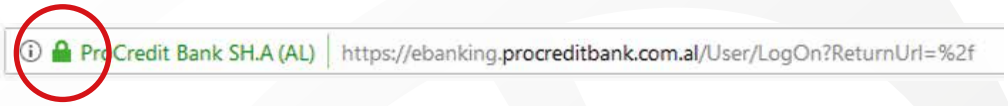
› Make sure you are using the official bank app

One of the safest ways to conduct bank transactions is through the ProCredit official mobile app. For this purpose, you may use also the web browser, but the app ensures advanced encryption level.

› Always make sure you know the person you communicate with

• Before inserting any information, always check the presence of the lock icon on top of the window which indicates the webpage you are accessing. If the webpage is safe, you will see the bank address change from “http” to “https”.
• You may be sure about the ProCredit Bank security certificate by clicking on the lock icon appearing on top of the window which indicates the webpage name.

Mozilla Firefox:



Internet Explorer:

Google Chrome:

› Save your password safely

• Always memorize your passwords and any other security information. Destroy any documents by which this information was conveyed to you, in order to prevent this information from being used by third parties.
• Take the required steps to save the password and security information. Do not disclose this information to any relative, friends or anybody.
• Whenever you call the bank, you must know that the bank will never ask for your password over the phone.
• Make sure that you log out properly from e-banking/m-banking after you complete your transactions.
• Never store your password in your computer (via password manager). You may do this only when certain that your computer is fully protected.
• Never leave your electronic devices unattended while logged on e-banking/m-banking.
• We recommend that you change your password regularly. Always chose a password that cannot be easily found.
• Do not use e-banking/m-banking password in other internet pages.

Part of the ProCredit Group

ProCredit Bank

Additional measures

› Protect your electronic devices

• Be careful from e-mails you receive from strangers and never click on links in these e-mails to access any website.
• Never open, download or execute documents attached to e-mails sent by strangers which you find suspicious or coming from an unreliable source.
• Install antivirus software and regularly update it and do security scanning. Install the latest security updates which in technical IT terms are called “patches”.

Consider any actions which you find unusual to your m-baking procedure as suspicious. Once this suspicion arises, contact ProCredit by visiting one of our service points, contact your advisor or call the ProCredit Bank Contact Centre +355 4 2 389 389.

February 2020 – Amendments might have been done from the date of production