



ProCredit Bank

Best and Safest Practices

in Executing Transactions with Your Cards



© 038 555 555 | 049 555 555 | www.procreditbank-kos.com



Having a card and PIN number

The use of the card bears values and advanced opportunities compared to cash, as definitely the security aspect is always on the side of the card. If the card is lost or stolen does not necessarily mean loss of money if it is used pursuant to the best security practices. A card is a tool that enables payments and withdrawals of cash, therefore treat you card with due care just as you treat your cash.

Do not allow for your card to be photocopied or photographed, please be careful as the front and back sides of card contain sensitive data, such as: card number, expiry date (front), three-digit code–CVV2 (back), etc., which may be misused if they fall in the hands of fraudsters. Keep your PIN secret and handle your card with due care. Memorize your PIN.

Do not save your card PIN or other data related to the card in your computer, mobile phone, or paper.

Do not allow under any circumstances that your PIN and your card are kept together.

Do not record or use your card PIN in such manner that it would enable it to be discovered by another person.

Do not tell anyone your card PIN (including bank employees, police, etc.)

ATM use

Be careful while using the ATMs, do not execute any transaction if there is something unusual about that ATM, pay special attention to any device next to the card reader.

Cover the PIN board with the other hand while you enter the PIN; thus, you protect the PIN from other persons or unauthorized monitoring devices.

If while using the card you notice something unusual at the ATM and even if you have already started a transaction, cancel it and notify the ProCredit Bank Call Center.

Avoid using an ATM that looks suspicious or unusual in any way. When using an ATM, look for scratches, glue, or tape remains, as these may be indicators of criminal activity at the ATM.

Familiarize yourself with the look and feel of the ATM, its external look and standard signs. Do not accept help from strangers when operating an ATM with a card.

If your card gets confiscated by the ATM of another bank, please request that your card is temporarily blocked by notifying the Call Center. Never give your card to anyone, treat it as cash.



Use at POS (sales terminals)

Always protect your card, every time you hand it for a payment be present while your card is being used and do not permit that your card is removed from your view.

Once the transaction is over, a receipt shall be printed.

- In some stores, in addition to the PIN, you may be asked to sign the receipt.
- Please make sure that your name, transaction date, card number (last digits), and the invoiced amount are accurate before you sign the receipt, by comparing the amount with the one in the fiscal coupon.

You are suggested to always save the receipt and fiscal coupon until the payment is reflected in your account balance.

Be careful while using the POS terminals, do not execute any transactions if there is something unusual at that POS, pay special attention to any device nearby. Immediately inform the ProCredit Bank Call Center.

Cover the PIN board with your other hand while you enter the PIN, in this way you protect your PIN from unauthorized persons or devices, also from surveillance cameras that selling points may have installed.


Do not accept any help from strangers while operating your card at the POS.

Using on the Internet

While making purchases via the Internet, once you have entered your card details, please make sure your computer screen is fixed so that you are the only one who can look at it. try avoiding the use of public computers for purchases.

It is preferable that you get connected from your home or personal computer and make sure that your applications, e.g., 'Firewall' and Anti-Virus/Spyware/Malware are updated and active.

Do not respond to emails/phone calls requesting information about your bank account, PIN, iPIN, Internet password, even ProCredit Bank, VISA and MasterCard will never ask for such secret information via email or phone.

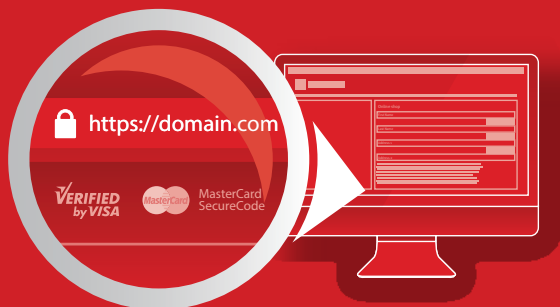


Should you receive such a request it can only be fraud, and in such cases notify immediately the ProCredit Bank Call Center.

Do not practice giving out the card number and CVV2 via phone or email, as this authorization method is very dangerous and may result in compromising the card. Apply for iPIN (Internet PIN and Internet password) to execute safer payments on all pages where you see the marks “MasterCard SecureCode” and “Verified by Visa”. For this service you may apply with each ProCredit Bank ATM.

When you make Internet purchases, select sellers (pages) that are credible and verify the safety features, such as: whether the Internet page has a security protocol (https://), the Internet security certificate is valid, etc. when you make Internet purchases do not click on links offered by ads or email with offers for Internet purchases or on other Internet pages. Instead, write yourself the address on the web browser.

Never open any attachments sent by someone you do not know. Treat every attachment you receive with caution even if you know who sent the email, and initially scan for viruses and then open or save that document.



Restrict publication of your personal data, e.g., personal number, passport number, full date of birth, card number, in any webpage, communication window or social media (e.g., Facebook, Twitter) or any other place in order to reduce the risk of your identity being stolen.

Do not give out the data of your card if you receive any offers via phone/email or phone SMS about any product / service / promotion or opportunity for investments that you did not initiate, but even if you did initiate it, before proceeding with the payment please undertake all measures to be on the safe side (verify the validity of the company, request for further documents, consult your bank etc.).

Anytime you make a payment or purchase via the Internet, please carefully read all terms and conditions the company has presented as by confirming and completing the payment you are completely subjected to those terms.

Please do not click the button “YES” on offers without payment or very cheap offers for products/services before you read all terms and conditions presented by the company. In the majority of cases, these offers integrate hidden fees and charges. In such cases you unknowingly may confirm registration for periodic fees/charges that are applied later.

Other details

CVV2 is the three-digit code placed only on the back side of your plastic card and serves as identification number for the card bearer when making online purchases, or during phone calls, therefore, please make sure you do not tell that to a third party.

iPIN means Internet PIN, and it serves to execute safer purchases on the Internet using the secure channel 3-D Secure, the Internet password serves to execute safer purchases on the Internet using the secure channel ‘3-D Secure’. To learn more about 3-D Secure please visit the ProCredit Bank (<http://www.procreditbank-kos.com/sq/3-D-Secure>) page.

On the Internet payment industry, the “YES” button is known as the client’s electronic signature, therefore by clicking on “YES” you agree with the terms and conditions defined for you.

Please make sure that your bank cards are signed immediately upon receipt and that you sign with a permanent pen on the signature panel on the back side of your card.

Your signature on the POS payment sheets must be identical with the one in your card. The signature identifies you as the card bearer and therefore, should be the same.

Please notify immediately the Call Center if you think someone may be aware of any of your secret card data; if you have lost it or if your card has been stolen.

If your card has expired, please destroy it completely.

Make sure that the ProCredit Bank always is in possession of the correct phone or mobile number and personal e-mail, so in case any suspicious activity is recorded in your account we may contact you. However, even in such cases we shall never ask you to share your secret data such as: card PIN, CVV2, iPIN and Internet password.

To be able to check the activity in your account more efficiently, we strongly advise you to:

- Regularly check your accounts.
- Activate the SMS notification about your transactions.

In case you notice any unauthorized transaction in the account or have received by SMS any notification about any unauthorized transaction, please contact immediately the ProCredit Bank Call Center.



