საბარათე ინსტრუმენტით სარგებლობის წესი და რეკომენდაციები

ტერმინთა განმარტებები:

- **საბარათე ინსტრუმენტი** – საგადახდო ინსტრუმენტი, მათ შორის, საგადახდო ბარათი, მობილური ტელეფონი, კომპიუტერი ან სხვა ტექნოლოგიური მოწყობილობა, რომელშიც ჩაწერილია/ინტეგრირებულია შესაბამისი საგადახდო აპლიკაცია და რომლის საშუალებით გადამხდელს შეუძლია განახორციელოს საბარათე ოპერაციის ინიციირება;

- **საბანკო ბარათი (შემდგომში - ბარათი)** - ბანკის მიერ კლიენტისთვის დამზადებული საგადახდო ინსტრუმენტი, რომელიც ბანკის საკუთრებაა და რომელიც განკუთვნილია კლიენტის მიერ სხვადასხვა საბანკო ოპერაციების საწარმოებლად (ბანკის მიერ გამოშვებული „ვიზა“ (VISA) ან „მასტერქარდ“ (MasterCard) ბარათი);
- **ვირტუალური ბარათი** – ბარათის ფიზიკურად არსებობის გარეშე ბარათის რეკვიზიტების (სულ მცირე, ბარათის ნომერი, მოქმედების ვადა და უსაფრთხოების კოდი) ერთობლიობა, რომლის საშუალებით ავთენტიფიკაციის შესაბამისი ზომების დაცვით ბარათის მფლობელს შეუძლია განახორციელოს გადახდები.
- **PIN კოდი** - პერსონალური საიდენტიფიკაციო ნომერი, ოთხი ციფრისგან შემდგარი პაროლი
- **CVV კოდი** - ბარათის მეორე მხარეს დატანილი სამი ციფრისგან შემდგარი ბარათის ვერიფიკაციის კოდი

უსაფრთხოების ძირითადი წესები

- ბანკის სერვისცენტრში ბარათის მიღებისას დარწმუნდით, რომ ბარათის **PIN კოდი** მოთავსებულია კონვერტში. კონვერტი არ უნდა იყოს დაზიანებული ან გახსნილი იმგვარად, რომ **PIN კოდი** ხილვადი იყოს სხვებისთვის. იმ შემთხვევაში, თუ კონვერტი დაზიანებული ან გახსნილია, შეატყობინეთ ბანკის ქოლ ცენტრს (+ 995 32) 2008080 / მობილურიდან * 8080
- მიღებული **PIN კოდი** დაიმახსოვრეთ, ხოლო კონვერტი გაანადგურეთ.
- სასურველია **PIN კოდი** შეცვალოთ თქვენთვის მისაღები ციფრების კომბინაციით ბანკის სერვისცენტრებში განთავსებულ ბანკომატში.
- იმ შემთვევაში თუ ვერ ახერხებთ **PIN კოდის** დამახსოვრებას, არავითარ შემთხვევაში არ შეინახოთ ჩაწერილი **PIN კოდი** ბარათთან ერთად და არ დააწეროთ კოდი ბარათზე. ჩაწერილი სახით **PIN კოდი** შეინახეთ მესამე პირებისთვის (მათ შორის მეგობრებისთვის, ნათესავებისთვის და ოჯახის წევრებისთვის) მიუწვდომელ ადგილას.
- სერვისცენტრში ბარათის მიღებისას, მოაწერეთ ხელი ბარათის უკანა მხარეს, ხელმოწერისთვის განკუთვნილ ველში.
- არასოდეს გაუზიაროთ მესამე პირებს (მათ შორის მეგობრებს, ნათესავებს, ოჯახის წევრებს) ბარათის სრული ნომერი, მოქმედების ვადა, **PIN კოდი**, **CVV კოდი**. განსაკუთრებული ყურადღებით იმოქმედეთ თუ გთხოვენ აღნიშნული ინფორმაციის გაზიარებას ტელეფონის, ელ.ფოსტის, სოციალური ქსელის საშუალებით და მისთ. არ გააზიაროთ ინფორმაცია იმ შემთხვევაშიც კი, თუ ინფორმაციის მომთხოვნმა წარადგინა თავი, როგორც ბანკის თანამშრომელმა. ასეთ შემთხვევებში, თავად დარეკეთ ბანკში და შეატყობინეთ აღნიშნული შემთხვევის შესახებ ქოლცენტრის თანამშრომელს (+ 99532) 2008080 / მობილურიდან *8080.
- ყურადღებით მოეკიდეთ ელექრონულ წერილებს, რომელსაც იღებთ სამსახურეობრივ, ან პირად მისამართზე. არასოდეს გადახვიდეთ ბმულებზე საეჭვო ელექტრონულ წერილში, თუ წერილი ითხოვს ბარათის ნომრის, **PIN კოდის**, **CVV კოდის**, კოდური სიტყვის, ინტერნეტ ბანკის მომხარებლის სახელის, პაროლის ან სხვა კონფიდენციალური ინფორმაციის გაზიარებას. ხშირ შემთხვევაში ბმულებიდან ხდება გადამისამართება ვებგვერდზე, რომელიც გამოიყენება ინფომაციის არასანქცირებულად მოპოვებისთვის.
- გახსოვდეთ, რომ ბანკი არასოდეს სთხოვს კლიენტებს კონფიდენციალური ინფორმაციის

მიწოდებას ელექტრონული ფოსტის ან რაიმე სხვა ფორმით.

- გახსოვდეთ, რომ ბარათი არის თქვენი ანგარიშის მართვის საშუალება. შესაბამისად, **PIN კოდის** მესამე პირებისთვის გაზიარების ან ბარათის დაკარგვის შემთხვევაში არსებობს თქვენი ფულადი სახსრების არასანქცირებული გამოყენების ალბათობა მესამე პირების მხრიდან.
- იმ შემთხვევაში, თუ გაქვთ ეჭვი, რომ თქვენი ბარათის **PIN კოდი**, ნომერი, მოქმედების ვადა, **CVV კოდი** ცნობილი გახდა მესამე პირებისთვის, ან თუ დაკარგეთ ბარათი, დაუყონებლივ დაუკავშირდით ბანკს და შეატყობინეთ ამის შესახებ. ბანკის ქოლცენტრის თანამშრომელი დაგეხმარებათ საჭირო ზომების მიღებაში. (+ 99532) 2008080 / მობილურიდან *8080
- არ დაუშვათ მესამე პირების მხრიდან თქვენი ბარათის ასლის გადაღება (კოპირება), ან სურათის გადაღება. არასდროს გააგზავნოთ თქვენი ბარათის დასკანირებული გამოსახულება ელექტრონული ფოსტის ან ე.წ. მესინჯერების საშუალებით, არ გააზიაროთ სოციალურ ქსელებში.

ბარათის გამოყენება ბანკომატში

- ბანკომატით სარგებლობისას მიაქციეთ ყურადღება, ხომ არ არის დამონტაჟებული ბანკომატზე დამატებითი მოწყობილობები. განსაკუთრებული ყურადღება მიაქციეთ **PIN კოდის** შესაყვან კლავიატურას და ბარათის მიმღებს. თუ შეამჩნიეთ არასწორად დამონტაჟებული კლავიატურა, ბარათის მიმღებზე დამონტაჟებული ე.წ. სქიმერი, უმჯობესია უარი თქვათ ბანკომატის გამოყენებაზე და მოიძიოთ ალტერნატიული ბანკომატი. შეატყობინეთ ბანკომატის მფლობელ ბანკს თქვენი ეჭვის შესახებ, როგორ წესი ბანკომატზე მითითებულია საკონტაქტო ინფორმაცია.
- PIN კოდის აკრეფისას დააფარეთ ხელი კლავატურას ისე, რომ გვერდზე მდგომებს არ ჰქონდეთ საშუალება დაინახონ თუ რა კოდი შეგყავთ. გაითვალისწინეთ, რომ **PIN კოდის** რამდენჯერმე არასწორად შეყვანისას, ბანკომატი დააკავებს ბარათს.
- ოპერაციის დასრულებისთანავე დაუყოვნებლივ ამოიღეთ ბარათი, ფულადი სახსრები და ქვითარი ბანკომატიდან. გადათვალეთ თანხა ადგილზე, დარწმუნდით, რომ ბანკომატმა დააბრუნა თქვენი ბარათი, დაელოდეთ ქვითარს (თუ მოითხოვეთ), შემდეგ მოათავსეთ თანხა და ბარათი უსაფრთხო ადგილას (ჩანთაში, საფულეში) და შემდეგ დატოვეთ ბანკომატი.
- არასოდეს ისარგებლოთ ბარათით ბანკომატებში მესამე პირების მხრიდან ტელეფონის საშუალებით მიღებული მითითებების საფუძველზე. არ დაუშვათ გარეშე პირების მონაწილეობა თქვენს მიერ განხორციელებულ ოპერაციებში და ყურადღებით მოეკიდეთ უცხო პირების რჩევას ბანკომატით სარგებლობასთან დაკავშირებით.
  - სასურველია, შეინახოთ ბანკომატში შესრულებული ოპერაციების ქვითრები საბანკო ანგარიშის ამონაწერთან შემდგომი შედარებისთვის.
- იმ შემთხვევაში, თუ ბანკომატმა არ დააბრუნა (დააკავა) ბარათი, დაუყოვნებლივ უნდა დაუკავშირდეთ ბანკს. (+ 99532) 2008080 / მობილურიდან *8080

ბარათის გამოყენება სავაჭრო ობიექტებში

- გამოიყენეთ ბარათი უნდაღდო ანგარიშსწორებისას მხოლოდ სანდო სავაჭრო ობიექტებში.
- ყოველთვის მოითხოვეთ ოპერაციის შესრულება თქვენი თანდასწრებით, არ გაატანოთ ბარათი თქვენგან მოშორებით სავაჭრო ან მომსახურების ობიექტის მომსახურე პერსონალს. ეს შეამცირებს თქვენი ბარათის მონაცემების არასანქცირებული მოპოვების რისკს.
- ბარათით ანგარიშსწორებისას, სავაჭრო ან მომსახურების ობიექტის თანამშრომელმა შესაძლოა მოგთხოვოთ პირადობის დამადასტურებელი საბუთი, **PIN კოდის** შეყვანა POS ტერმინალზე ან/და ქვითრის ხელმოწერა. **PIN კოდის** აკრეფისას დარწმუნდით, რომ ვერავინ ხედავს მას. თუ POS ტერმინალი არ არის აღჭურვილი კლავიატურის დამცველი მოწყობილობით, **PIN კოდის** აკრეფისას დააფარეთ კლავიატურას ხელი. სანამ მოაწერთ ხელს ქვითარს (მოთხოვნის შემთხვევაში) და დატოვებთ სავაჭრო ან მომსახურების ობიექტს, გადაამოწმეთ რამდენად შეესაბამება ჩეკზე მითითებული თანხა ოპერაციის თანხას.

- იმ შემთხვევაში თუ POS ტერმინალმა უარყო ოპერაცია, შეინახეთ უარყოფის ქვითარი საბანკო ანგარიშის ამონაწერთან შემდგომში შედარებისთვის.
- ზოგიერთ სავაჭრო და მომსახურების ობიექტებში, თანამშრომელი დამატებით ითხოვს თქვენი საბანკო ბარათის გატარებას კლავიატურაზე დამონტაჟებულ ბარათის წამკითხველში, რომელიც არ არის სერტიფიცირებული საერთაშორისო საგადამხდელო სისტემების (Visa, MasetCard) მიერ. გადაამოწმეთ წინასწარ, აპირებს თუ არა სავაჭრო ობიექტის მომსახურე პერსონალი, თქვენი ბარათის POS ტერმინალის გარდა სხვა მოწყობილობაში გატარებას. ასეთ შემთხვევაში გააფრთხილეთ პერსონალი, რომ მათ შეუძლიათ გამოიყენონ მათთვის სპეციალურად გადაცემულ ე.წ. სატესტო ბარათი, რომელიც საშუალებას მისცემს გადახდის პროცესის დასრულებას. თქვენი ბარათის კონფიცენციალური მონაცემები კი არ იქნება საეჭვო მოწყობილობაში დაფიქსირებული.

ბარათის გამოყენება ინტერნეტში

- ინტერნეტში ვაჭრობისთვის გამოიყენეთ მხოლოდ ცნობილი და სანდო საიტები. თუ ოდნავ ეჭვი შეგეპარებათ რომელიმე ვებ-გვერდის სანდოობაში, შეგიძლიათ გადაამოწმოთ მისამართი შემდეგ მისამართზე: http://www.scamadviser.com
- ონლაინ ოპერაციებისთვის არ გამოიყენოთ **PIN კოდი**. როგორც წესი, ონლაინ ოპერაციებისთვის საკმარისია ბარათის ნომერი, მოქმედების ვადა, ბარათის მფლობელის სახელი, გვარი და **CVV კოდი**.
  - ინტერნეტ ოპერაციებისთვის სასურველია გამოიყენოთ ცალკე ბარათი (მაგ,**ვირტუალური ბარათი**, ან e-card), სადაც სახსრების განთავსება უნდა მოხდეს საჭიროებისამებრ - ოპერაციის უშუალოდ შესრულების წინ.
- ყოველთვის ყურადღებით გადაამოწმეთ ვებ გვერდის მისამართი, სადაც შეგყავთ ბარათის მონაცემები. შესაძლოა სახეშეცვლილი მისამართები (რამოდენიმე სიმბოლოს ცვლილებით) სპეციალურად იყოს შექმნილი ბარათის მონაცემების არასანქცირებული მოპოვებისთვის. ვებ გვერდის ვალიდურობის შემოწმება შესაძებელია ვებ-გვერდის სერტიფიკტის გადამოწმებით (როგორც წესი ბოქლომის გამოსახულებაზე დაჭერით).

ვებ- გვერდის სერტიფიკატის გადამოწმება

- ინტერნეტ ვაჭრობისთვის სასურველია გამოიყენოთ მხოლოდ პირადი კომპიუტერი ან მობილური მოწყობილობა, ეს შეამცირებს თქვენი პირადი კონფიდენციალური ინფორმაციის გამჟღავნების ალბათობას.
- ინტერნეტში ვაჭრობისას არ ისარგებლოთ საჯარო ან თქვენთვის უცნობი WiFi ინტერნეტ ქსელით.
- იმ შემთხვევაში, თუ ონლაინ ოპერაციებისთის იყენებთ საერთო წვდომის ან სხვა პირის კუთვნილ კომპიუტერს, ოპერაციის შესრულებისას არ დაიმახსოვროთ ბარათის მონაცემები და ოპერციის დასრულების შემდეგ წაშალეთ მონაცემები.
- თქვენს კუთვნილ კომპიუტერზე ან მობილურ მოწყობილობაზე აუცილებლად დააყენეთ ანტივირუსული პროგრამული უზრუნველყოფა. რეგულარულად მოახდინეთ ანტივირუსის, მოწყობილობის ოპერაციული სისტემის და სხვა პროგრამების განახლებები. ეს შეამცირებს თქვენს კომპიუტერში ვირუსების მოხვედრის ალბათობას.
- დამატებით გაეცანით ბანკის კიბერუსაფრთხოების შესახებ ინფორმაციას ბმულზე: https://www.cartubank.ge/ge/612/