საბანკო ბარათებისა და ფიშინგის უსაფრთხოების სქემები

დანაშაულის ერთ-ერთი ყველაზე გავრცელებული ფორმა არის **ფიშინგი.**

ფიშინგი არის კიბერდანაშაულის ფორმა, რომლის მიზანია თაღლითური გზით ინტერნეტ მომხმარებლის პერსონალური მონაცემების მოპოვება. მაგალითად, კიბერთაღლითები აყალბებენ ცნობილი კომპანიების ვებ-გვერდებს ან უგზავნიან შეტყობინებებს მათი სახელით სხვადასხვა დისტანციური არხით, სადაც მომხმარებელს სთხოვენ პერსონალური მონაცემების (პაროლი, ბარათის ნომერი და ა.შ) შეყვანას და მრავალი სხვა.

საბანკო ბარათის გამოყენება გაცილებით უსაფრთხო, მოსახერხებელი და საიმედოა, ვიდრე ნაღდი ფულით სარგებლობა. თუმცა, თუ არ დავიცავთ უსაფრთხოების ზოგად წესებს, შესაძლოა ჩვენ თვითონვე მივცეთ საშუალება გამოიყენონ ჩვენი ბარათი და მასზე არსებული ხელმისაწვდომი თანხა.

ქვემოთ მოცემული რეკომენდაციები დაგეხმარებათ მაქსიმალურად დაიცვათ თავი, აგრეთვე შეამცირებს სავარაუდო რისკებს ნებისმიერი განხორციელებული ოპერაციის დროს:

- ბანკომატით სარგებლობისას
- უნაღდო ანგარიშსწორების დროს, პოს-ტერმინალით
- ინტერნეტის ქსელში
- ინტერნეტ და მობაილ ბანკში და ა.შ.

იმისთვის, რომ თავი დაიცვათ თაღლითობისგან:

- არ შეიყვანოთ პირადი ინფორმაცია საეჭვო ვებ-გვერდზე
- ნუ ენდობით მეილებს, რომლებიც თქვენგან პირადი ინფორმაციის ან საბანკო დეტალების შეყვანას ითხოვს. თქვენი ბანკი არასდროს მოგთხოვთ სენსიტიურ ინფორმაციას ელ-ფოსტით
- არ ენდოთ შეტყობინებებს, რომლებშიც თქვენგან სასწრაფოდ ითხოვენ რაიმე ქმედებას. სასწრაფოობა ხშირად იმის ნიშანია, რომ კიბერდამნაშავესთან გაქვთ საქმე;
- დააკვირდით ვებ-გვერდს, თუ იგი ნაკლებ პროფესიონალურად გამოიყურება ან შეიცავს შეცდომებს, შესაძლოა გამომგზავნი კიბერდამნაშავეა
- გახსოვდეთ, რომ კიბერდამნაშავე თქვენთვის კარგად ნაცნობი იმიჯით ცდილობს თქვენს მოტყუებას. შესაბამისად, აუცილებელია გადაამოწმოთ ყველაფერი, რაც საეჭვოდ მოგეჩვენებათ. მხოლოდ ასე შეძლებთ რისკების მინიმუმამდე შემცირებას

უკონტაქტო საბარათე გადახდების პირობები:

გაცნობებთ, რომ საქართველოს ეროვნული ბანკის რეგულაციის შესაბამისად 1.05.23-დან ძალაში შევიდა საგადახდო ბარათით უკონტაქტო გადახდისას ვერიფიკაციის წესის შესახებ ცვლილება, კერძოდ, ნებისმიერი ბარათით უკონტაქტოდ შესრულებული ტრანზაქციისას ჯამურად მიყოლებით გახარჯულ ყოველ 600 ლარზე დაგჭირდებათ პინ-კოდით ვერიფიკაცია.

გთხოვთ გაითვალისწინოთ:

- ათვლაში მონაწილეობს 1 მაისამდე შესრულებული უკონტაქტო ოპერაციები.
- ათვლა ნულდება მაშინ, როდესაც შესრულდება პირველი პინ-კოდიანი ოპერაცია (მაგ. ბანკომატით თანხის განაღდების ოპერაცია)
- ათვლაში არ მონაწილეობს ელექტორნული საფულით: Google Pay, Apple Pay გადახდები
- ათვლაში არ მონაწიელეობს ისეთი ოპერაციები სადაც არ ხდება თანხის ხელით კორექტირება, მაგ. პარკინგი და ა.შ.
- ათვლაში არ მონაწილეობს მცირე მოცულობიანი თანხები - კერძოდ, 10 ლარამდე ოპერაციები.

უკონტაქტოდ პინის ვერიფიკაციის გარეშე გადახდის ლიმიტი კვლავაც განისაზღვრება 100 ლარით.

ზოგადი რეკომენდაციები:

- არასოდეს გადასცეთ თქვენი ბარათის პინ–კოდი მესამე პირს, მათ შორის ნათესავებს, ნაცნობებს, თანამშრომლებს, საკრედიტო ორგანიზაციების თანამშრომლებს, მოლარეებს და აგრეთვე იმ პირებს, ვინც დახმარებას გიწევთსაბანკო ბარათის გამოყენებისას.
- პინ-კოდი სასურველია შეცვალოთ თქვენთვის ადვილად დასამახსოვრებელი კომბინაციით.
- არასდროს გადასცეთ ბარათი მესამე პირს.
- შემომავალი სატელეფონო ზარის ან ელექტრონული წერილისმიღებისას არ გასცეთ თქვენი ბარათის მონაცემები იმ შემთხვევაშიც კი, თუ წარდგენა მოახდინეს, როგორც თქვენი მომსახურე ბანკის თანამშრომელი.
- დარწმუნდით, რომ გააქტიურებული გაქვთ სმს სერვისი ტრანზაქციებთან დაკავშირებით.
- ბარათის დაკარგვის ან მოპარვის შემთხვევაში, დროულად დაბლოკეთ ბარათი დისტანციური სერვისების (ინტერნეტ/მობაილ ბანკი) დახმარებით, ან შეატყობინეთ ბანკს ქოლ-ცენტრის მეშვეობით +995 32 2 42 42 42

რეკომენდაციები საბანკო ბარათის ბანკომატში გამოყენების დროს:

- პინის აკრეფისას დარწმუნდით, რომ იგი არ არის ხილვადი გვერდზე მდგომი მესამე პირისთვის.
- ქვეყნის გარეთ ეცადეთ განახორციელოთ ოპერაცია იმ ბანკომატებში, რომლებიც განთავსებულია ბანკის ფილიალებში, სახელმწიფო ორგანიზაციებში, დიდ სავაჭრო ცენტრებში, სასტუმროებში, აეროპორტებში და ა.შ.
- ყურადღებით გაეცანით ბანკომატზე გამოტანილ შეტყობინებას (ასეთის არსებობის შემთხვევაში), რადგან ის შეიძლება გაცნობდეთ დამატებითი მომსახურების საკომისიოს შესახებ.
- ბანკომატის ან ტერმინალის მომსახურე მხარემ შესაძლოა კრედო ბანკისგან დამოუკიდებლად შემოგთავაზოთ განაღდების ოპერაციის განსხვავებულ ვალუტაში ანგარიშსწორება, განურჩევლად იმისა, თუ რა ვალუტას გასცემს ბანკომატი ფიზიკურად ან რა ვალუტა გაქვთ ხელმისაწვდომი ბარათზე. შემოთავაზებაზე თანხმობის დაფიქსირების შემთხვევაში ოპერაცია დამუშავდება ბანკომატის მიერ განსაზღვრული კურსით, რამაც შეიძლება გამოიწვიოს თქვენთვის მნიშვნელოვანი ხარჯი, ამიტომ დააკვირდით შემოთავაზებულ გაცვლით კურსს და გააკეთეთ სასურველი არჩევანი.

რეკომენდაციები საბანკო ბარათის ინტერნეტ ქსელში გამოყენებისას:

- უმჯობესია ინტერნეტ ქსელში საბანკო ბარათი გამოიყენოთ მხოლოდ თქვენს პირად კომპიუტერში, რადგანარსებობს კონფიდენციალური ინფორმაციის დამახსოვრების რისკი.
- ბარათი გამოიყენეთ მხოლოდ სანდო და ცნობილ ინტერნეტ საიტებზე.
- არ ენდოთ დაუჯერებლად მიმზიდველ შემოთავაზებას.
- ლინკზე დაჭერით გახსნილ ვებ-გვერდზე არ შეიყვანოთ ინტერნეტ ბანკის მომხმარებელი და პაროლი.
- ყოველთვის თავად აკრიფეთ ინტერნეტ ბანკის მისამართი.

რეკომენდაციები საბანკო ბარათის სავაჭრო ობიექტში გამოყენებისას (პოს-ტერმინალი):

- არასოდეს გაატანოთ ბარათი მომსახურე პერსონალს მათ შორის რესტორანში ან ბენზინ/გაზ გასამართ სადგურში.
- მოითხოვეთ ბარათით ოპერაციის ჩატარება მოხდეს თქვენი თანდასწრებით, რათა შემცირდეს ბარათიდან მონაცემების უკანონო დაუფლების რისკი.
- გადაამოწმეთ განაღდებული თანხის ოდენობა სმს შეტყობინებაში ან ქვითარზე.

ფიშინგი:

გვინდა გაგიზიაროთ რჩევები, თუ როგორ უნდა დაიცვათ თავი ონლაინ კიბერთაღლითობისგან. დანაშაულის ერთ-ერთი ყველაზე გავრცელებული ფორმა არის ფიშინგი.

ფიშინგი არის კიბერდანაშაულის ფორმა, რომლის მიზანია თაღლითური გზით ინტერნეტ მომხმარებლის პერსონალური მონაცემების მოპოვება.

მაგალითად: კიბერთაღლითები აყალბებენ ცნობილი კომპანიების ვებ-გვერდებს ან უგზავნიან შეტყობინებებს მათი სახელით სხვადასხვა დისტანციური არხით, სადაც მომხმარებელს სთხოვენ პერსონალური მონაცემების (პაროლი, ბარათის ნომერი და ა.შ) შეყვანას.

იმისთვის, რომ თავი დაიცვათ აღნიშნული თაღლითობისგან:

- არ შეიყვანოთ პირადი ინფორმაცია საეჭვო ვებ-გვერდზე;
- ნუ ენდობით მეილებს, რომლებიც თქვენგან პირადი ინფორმაციის ან საბანკო დეტალების შეყვანას ითხოვს. თქვენი ბანკი არასდროს მოგთხოვთ სენსიტიურ ინფორმაციას ელ-ფოსტით;
- არ ენდოთ შეტყობინებებს, რომლებშიც თქვენგან სასწრაფოდ ითხოვენ რაიმე ქმედებას. სასწრაფოობა ხშირად იმის ნიშანია, რომ კიბერდამნაშავესთან გაქვთ საქმე;
- დააკვირდით ვებ-გვერდს, თუ იგი ნაკლებ პროფესიონალურად გამოიყურება ან შეიცავს შეცდომებს, შესაძლოა გამომგზავნი კიბერდამნაშავეა.

გახსოვდეთ, რომ კიბერდამნაშავე თქვენთვის კარგად ნაცნობი იმიჯით ცდილობს თქვენს მოტყუებას. შესაბამისად, აუცილებელია გადაამოწმოთ ყველაფერი, რაც საეჭვოდ მოგეჩვენებათ. მხოლოდ ასე შეძლებთ რისკების მინიმუმამდე შემცირებას.

დაიცავით უსაფრთხოების ზოგადი წესები და იყავით მშვიდად, რადგან თქვენი ბარათი თქვენსავე საიმედო ხელშია!