საკრედიტო ბარათის უსაფრთხოება

- ბარათის ინფორმაცია არ უნდა მოხვდეს უცხო პირების ხელში.
- ბარათის გადახდისას მომხმარებელმა არ უნდა გაატანოს ბარათი მომსახურე პერსონალს, უნდა მოითხოვოს ტერმინალის ადგილზე მოტანა.
- ბარათზე არსებული CVC კოდი მომხმარებელს შეუძლია დაიმახსოვროს და ბარათიდან წაშალოს.
- ინტერნეტ შოპინგისთვის და ყოველდღიური ხმარებისთვის რეკომენდებულია მომხმარებელს ჰქონდეს სხვადასხვა ბარათი.

რეკომენდაციები

- არ შეიყვანოთ ბარათის მონაცემები საეჭვო ვებგვერდებზე, რომლებიც არ იწყება https და არ აქვს ბოქლომის ნიშანი ან გააჩნია ორიგინალისგან განსხვავებული დასახელება.
- მოერიდეთ საჯარო wifi-ის გამოყენების დროს საბანკო ოპერაციების შესრულებას.
- მოერიდეთ ბარათის მონაცემების დამახსოვრებას ვებგვერდებზე ანგარიშსწორებისას.
- არ შეინახოთ ბარათის მონაცემები მობილურ ტელეფონში და არ გადაუღოთ მას სურათი.
- არ უკარნახოთ სხვა პირებს თქვენი ბარათის მონაცემები.
- ჩართეთ 3D მომსახურების სერვისი და დაადასტურეთ გადახდები SMS-ით.
- ჩართეთ SMS მომსახურება და აკონტროლეთ თითოეული ოპერაცია.
- დაბლოკეთ ბარათი საეჭვო ოპერაციის დაფიქსირებისას და მიმართეთ ოპერატორს დასახმარებლად.

ფიშინგი

ფიშინგი არის კიბერთაღლითობის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლს მოტყუების გზით მოპაროს სენსიტიური ინფორმაცია ან მოახდინოს კომპიუტერის კომპრომეტაცია. შეტევის დროს გამოიყენება მეილი, რომელიც იგზავნება კიბერ-კრიმინალების მიერ. ძირითადად, მეილი წარმოჩენილია როგორც სანდო წყაროსგან მიღებული შეტყობინება, როგორიცაა ბანკი ან ნებისმიერი სხვა ორგანიზაცია თუ პირი ვისთანაც მსხვერპლს შესაძლოა ქონდეს ურთიერთობა. მეილი შენიღბულია როგორც სასწრაფო შეტყობინება, რომელშიც დამატებითი ინფორმაციისთვის მოთავსებულია ვებ-ბმულები ან მიმაგრებული დოკუმენტები. ფიშინგ მეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად შესაძლებელია მოხდეს მსხვერპლის კომპიუტერში შეღწევა ან მისგან დამატებით სენსიტიური ინფორმაციის მოთხოვნა (პაროლი, მომხმარებლის სახელი, ბარათის ინფორმაცია და სხვა). კიბერ-დამნაშავეები ცდილობენ ფიშინგ მეილები დააგზავნონ მასიურად, მაქსიმალურად მეტ ადრესატთან, რაც მათი წარმატების ალბათობას რეალურს ხდის.

როგორ დავიცვათ თავი ფიშინგისგან?

პირველ რიგში უნდა გავიაზროთ, რომ გარკვეულ დროს შეიძლება ნებისმიერი ჩვენგანი გახდეს ფიშინგის მსხვერპლი. ფიშინგ შეტევის წარმატების ალბათობა უფრო მაღალია, როდესაც მსხვერპლზე არსებობს პირადი ინფორმაცია (სად მუშაობს, რომელი ბანკის მომხმარებელია, რომელ მაღაზიებში დადის, სად ცხოვრობს, ინტერესის სფერო და სხვა). მას შემდეგ რაც გაათვითცნობიერებთ, რომ ნებისმიერ მომენტში შეიძლება თქვენც

აღმოჩნდეთ შეტევის მსხვერპლი, მნიშვნელოვანია იცოდეთ ფიშინგისგან დაცვის საშუალებები:

- არ შეიყვანოთ პირადი ინფორმაცია საეჭვო ვებ-გვერდზე
- პირადი ინფორმაციის, მაგალითად ბარათის მონაცემების ინტერნეტში შეყვანისას, ყოველთვის დააკვირდით, რომ იმყოფებით დაცულ გვერდზე. დაცული გვერდი იწყება ასე https:// და აქვს ბოქლომის ნიშანი
- მაქსიმალურად შეზღუდეთ ინფორმაციის (რომელმაც თქვენს შესახებ შესაძლებელია დამატებითი დეტალები მიაწოდოს უცხო პირს) გაზიარება სოციალურ ქსელში, Facebook-ზე, ფორუმებზე და სხვა ინტერნეტ რესურსებზე. რაც უფრო მეტ პერსონალური ტიპის ინფორმაცია იქნება ხელმისაწვდომი საჯაროდ თქვენზე, მით უფრო გაუადვილდება კიბერ-დამნაშავეს თქვენი მახეში გაბმა.
- თუ მიიღებთ მეილს, რომელიც გთხოვთ რომ გადახვიდეთ ვებ-ბმულზე ან გახსნათ მიმაგრებული დოკუმენტი, გადაამოწმეთ შეტყობინება. თუ მეილი წარმოჩენილია როგორც ნაცნობი ორგანიზაციისგან ან პირისგან გამოგზავნილი, გადაამოწმეთ შესაბამისი ორგანიზაციის ან პირის საკონტაქტო დეტალები, რომელიც თქვენთვის არის ცნობილი.
- ნუ ენდობით მეილებს, რომლებიც თქვენგან პირადი ინფორმაციის ან საბანკო დეტალების შეყვანას ითხოვს. თქვენი ბანკი არასდროს მოგთხოვთ სენსიტიურ ინფორმაციას ელ-ფოსტით.
- გადაამოწმეთ ვებ-გვერდის მისამართი. გახსოვდეთ რომ „გაყალბებული" ვებ-გვერდის მისამართი შეიძლება მიმსგავსებული იყოს ორიგინალთან და შეცვლილი იყოს ერთი ან რამდენიმე სიმბოლო
- აუცილებლად გამოიყენეთ ანტივირუსი
- არ დააკლიკოთ ბმულს, დააკოპირეთ ის და ისე გადაიტანეთ მეილიდან ვებ-ბრაუზერში
- მიიტანეთ მაუსი ბმულთან, სადაც გამოჩნდება ბმულის რეალური მისამართი
- თუ წერილი გამოგზავნილია ნაცნობი ადამიანისგან, ეს იმას არ ნიშნავს რომ ის არ იქნება საფრთხის შემცველი. შესაძლებელია თქვენი ნაცნობის კომპიუტერი დაინფიცირებული იყოს, რომელიც აგზანიდეს საფრთხის შემცველ წერილებს
- არ ენდოთ შეტყობინებებს, რომლებშიც თქვენგან სასწრაფოდ ითხოვენ რაიმე ქმედებას. სასწრაფოობა ხშირად იმის ნიშანია, რომ კიბერდამნაშავესთან გაქვთ საქმე
- გადაიკითხეთ ელ-ფოსტა. თუ ის ნაკლებად პროფესიონალურად გამოიყურება ან შეიცავს შეცდომებს, შესაძლებელია გამომგზავნი კიბერდამნაშავეა.

<u>უსაფრთხოების წესები ბანკომატის გამოყენებისას</u>

ბანკომატის გამოყენებასთან დაკავშირებული უსაფრთხოების რჩევები. თითოეული მათგანის გათვალისწინებით, მნიშვნელოვნად დაცულები იქნებით თაღლითების მიერ სხვადასხვა სახის გაყალბებისგან.

- ყოველთვის დააკვირდით ბანკომატის ირგვლივ არსებულ გარემოს. არ გამოიყენოთ ბანკომატი, თუ შენიშნავთ საეჭვო გარემოებას ან/და პირებს;
- ბანკომატის გამოყენება არ არის რეკომენდირებული, თუ ბანკომატის სპეციალური გარე განათების საშუალებები ცუდად ანათებს;

· ასევე არ გამოიყენოთ ის ბანკომატები, რომლებიც გამოიყურება უჩვეულოდ (ბანკომატს მიმარგერული აქვს რაიმე სახის უჩვეული/არასტანდარტული მოწყობილობა)

· ბანკომატის გამოყენებისას, ყოველთვის დადექით ბანკომატის კლავიატურის წინ ისე, რომ მესამე პირების თვალთახედვის არეში ვერ მოხვდეს თქვენი ბარათის PIN-კოდის შეყვანის ქმედება;

· ბანკომატზე, ბარათის PIN-კოდის შეყვანისას, ნუ მისცემთ მესამე პირებს საშუალებას, რომ თქვენი ზურგიდან დაინახონ ბანკომატზე თქვენს მიერ აკრეფილი PIN-კოდი. ყოველთვის დაიმახსოვრეთ თქვენი PIN-კოდი და არასდროს არ დაწეროთ თქვენი ბარათის PIN-კოდი, ბარათის უკანა მხარეს;

· იმ შემთხვევაში თუ, ბანკომატის გამოყენებით უნდა შეასრულოთ რამოდენიმე ოპერაცია, რეკომენდირებულია, რომ თანხის განაღდების ოპერაცია შეასრულოთ ყველაზე ბოლოს;

· ბანკომატის გამოყენების დასრულებისას, ყოველთვის დარწმუნდით, რომ:

- თქვენი ბარათი და თანხა (თანხის განაღდების ოპერაციის შესრულებისას) თქვენ გაქვთ;

- ნამდვილად დაასრულეთ თქვენს მიერ შესრულებული ოპერაცია. მაგალითად, თუ ბანკომატის ეკრანზე გამოვიდა შეტყობინება ,,გნებავთ სხვა ტრანზაქცია,, კლავიატურაზე ღილაკი ,,გაუქმება"-ს გამოყენებით დაასრულეთ ოპერაცია ან ეკრანზე განთავსებული გვერდითა ფუნქციონალური ღილაკი ,,არა" -ს გამოყენებით დაასრულეთ ოპერაცია.