ინტერნეტ უსაფრთხოების ინფორმაცია: “ფიშინგი”

რა არის “ფიშინგი”?

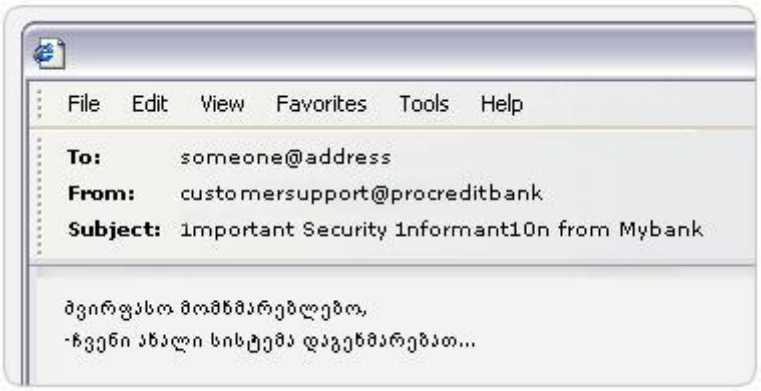
“ფიშინგი” არის სხვადასხვა შემთხვევით ადრესატებთან ელექტრონული ფოსტის გაგზავნა, რომელიც თითქოსდა გამოგზავნილია ინტერნეტში მოქმედი რეალური ორგანიზაციისგან, რომლის მიზანია მოტყუების გზით აიძულოს ამ ორგანიზაციის კლიენტები გაამჟღავნონ თავიანთი ინფორმაცია თაღლითების მიერ შექმნილ ყალბ ვებ–გვერდზე. ასეთი წერილი, როგორც წესი, იტყობინება, რომ აუცილებელია კლიენტის ანგარიშის "განახლება" ან "გადამოწმება" ელექტრონულ ფოსტაში მოცემული ბმულის საშუალებით, რომელიც ყალბ ვებ–გვერდზე გადადის. ყალბ ვებ-გვერდზე შეყვანილი ნებისმიერი ინფორმაცია თაღლითების ხელში გადადის, რომლებიც მას თავიანთი მიზნებისთვის იყენებენ.

როგორ ავირიდოთ “ფიშინგის” საფრთხე?

მთავარია, სიფრთხილით მოეკიდოთ თქვენს მიერ მიღებულ, ყველა უცნობ და მოულოდნელ ელექტრონული წერილს, თუნდაც ის ერთი შეხედვით საიმედო წყაროდან იყოს მოწერილი. წერილები შემთხვევით მისამართებზე იგზავნება, რეალურ კლიენტამდე მიღწევის იმედით, რომელსაც სამიზნე ბანკში ანგარიში აქვს გახსნილი.
მართლაც, "პროკრედიტ ბანკი" შეიძლება ელექტრონული ფოსტით დაგიკავშირდეთ, მაგრამ ამ შეტყობინებაში "პროკრედიტ ბანკი" არასდროს მოითხოვს თქვენგან ელექტრონულ ფოსტაში თქვენი პაროლის ან სხვა კონფიდენციალური ინფორმაციის გამჟღავნებას, ბმულზე დაწკაპუნებით ან ვებ–გვერდზე გადასვლის საშუალებით. გახსოვდეთ თუ რა გზით გიკავშირდებათ ხოლმე თქვენი ბანკი და არასდროს გაამჟღავნოთ თქვენი სრული პაროლი ან პირადი ინფორმაცია.

როგორ უნდა ამოიცნოთ თაღლითური "ფიშინგ" წერილი

1 – ვისგან მოვიდა ელექტრონული ფოსტა?



“ფიშინგ” წერილი შეიძლება გამოიყურებოდეს ისე, თითქოს ის ნამდვილად "პროკრედიტ ბანკის" ელექტრონული ფოსტის მისამართიდანაა მოსული. სამწუხაროდ, ინტერნეტ ფოსტის სტრუქტურის გამო, ფიშერებისათვის შედარებით ადვილია ყალბი ჩანაწერის შექმნა გამომგზავნის ველში.

ელექტრონული მისამართი, რომელიც მითითებულია გამომგზავნის ველში, არ არის იმის გარანტია, რომ წერილი შეტყობინებაში მითითებული პირის ან ორგანიზაციისგანაა მოსული. ასეთი წერილები, შესაძლოა არ იყოს გაგზავნილი საბანკო სისტემიდან.

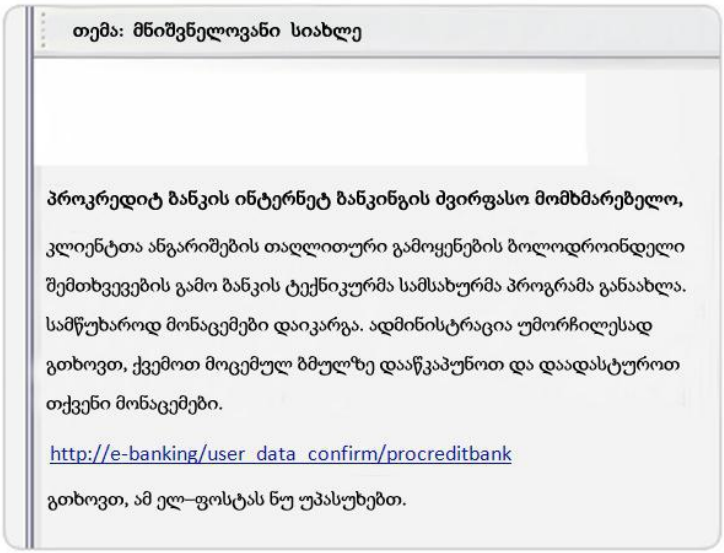
2 – ვისთვისაა განკუთვნილი ელექტრონული ფოსტა?

წერილები იგზავნება საერთო მისამართების სიაში მითითებულ ადრესატებთან. თაღლითებს ნაკლებად ეცოდინებათ თქვენი რეალური სახელი ან რაიმე სხვა ინფორმაცია თქვენს შესახებ, ასე რომ თქვენ ზოგადი სიტყვებით მოგმართავენ, მაგალითად, "ძვირფასო კლიენტო".

3 - ყურადღებით გაეცანით შეტყობინებას - აქვს თუ არა მას "ფიშინგის" ნიშნები?

პირველ რიგში, უნდა გახსოვდეთ, რომ ბანკები არასდროს მოგწერენ ელექტრონულ ფოსტას თქვენი პაროლის ან სხვა კონფიდენციალური ინფორმაციის გამჟღავნების მოთხოვნით. ველში "თემა" სავარაუდოდ იქნება უჩვეულო ან დიდი ზომის ასოები (ეს არის სპამ–ფილტრისგან თავის არიდების მცდელობა), მათ შორის გრამატიკული და ორთოგრაფიული შეცდომები.

თაღლითური შეტყობინების ნიმუში


თემა: მნიშვნელოვანი სიახლე

პროკრედიტ ბანკის ინტერნეტ ბანკინგის ძვირფასო მომხმარებელო,

კლიენტთა ანგარიშების თაღლითური გამოყენების ბოლოდროინდელი შემთხვევების გამო ბანკის ტექნიკურმა სამსახურმა პროგრამა განაახლა. სამწუხაროდ მონაცემები დაიკარგა. ადმინისტრაცია უმორჩილესად გთხოვთ, ქვემოთ მოცემულ ბმულზე დააწკაპუნოთ და დაადასტუროთ თქვენი მონაცემები.

http://e-banking/user_data_confirm/procreditbank

გთხოვთ, ამ ელ–ფოსტას ნუ უპასუხებთ.

არასდროს შეხვიდეთ თქვენ ინტერნეტ ბანკინგში ელექტრონული ფოსტის შეტყობინებაში მითითებულ ბმულზე დაწკაპუნებით.
ყოველთვის გახსენით ვებ ბრაუზერი და თავად შეიყვანეთ "პროკრედიტ ბანკის" ინტერნეტ ბანკინგის მისამართი.

თუ იმ შეტყობინების ნამდვილობასთან დაკავშირებით, რომელიც თითქოსდა "პროკრედიტ ბანკიდან" მოვიდა, რაიმე ეჭვები გაგაჩნიათ, დაუყოვნებლივ შეატყობინეთ "პროკრედიტ ბანკს" უახლოეს ფილიალში მისვლით, თქვენს კლიენტთა მრჩეველთან

დაკავშირებით ან შემდეგ ტელეფონის ნომერზე დარეკვით: (832) 2202222. შეგიძლიათ ასევე გადააგზავნოთ საეჭვო შეტყობინება შემდეგ საფოსტო მისამართზე: infosec@procreditbank.ge

4 - სად გაიხსნება ჰიპერბმული?

სამწუხაროდ, ძალიან ადვილია ბმულის რეალური დანიშნულების დამალვა, ასე რომ თქვენი ელექტრონული ფოსტის სტატუსის ველში ჩასმული ბმულის ან ნებისმიერი სხვა ინფორმაციის გაყალბება სირთულეს არ წარმოადგენს.

როგორ უნდა შენიშნოთ თაღლითური ვებგვერდი

რა არის საიტის მისამართი?

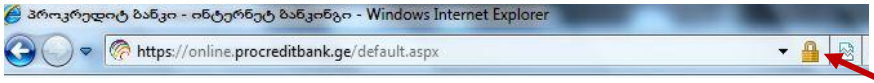
ელექტრონულ ფოსტაში ჩასმულ ბმულზე დაწკაპუნებით ვებ–გვერდზე გადასვლისას, სამისამართო ველიდან ყალბი ვებ–გვერდის რეალური ადგილმდებარეობის დადგენის მრავალი საშუალება არსებობს. ვებ–გვერდის მისამართი შეიძლება იწყებოდეს ნამდვილი გვერდის დომენის სახელით, მაგრამ არ არის იმის გარანტია, რომ ეს გვერდი ნამდვილია. არსებობს სხვა საშუალებებიც: რიცხვების შემცველი მისამართები, მსგავსი მისამართის დარეგისტრირება (როგორიცაა www.mybank-verify.com), ასევე ბრაუზერის ფანჯარაში ყალბი სამისამართო ველის ჩასმა. ამ გვერდებზე ბმულების უმეტესობა შეიძლება ნამდვილ ვებ–გვერდზე გადადიოდეს, ასე რომ არ მოტყუვდეთ.

იმისათვის, რომ დარწმუნდეთ, რომ "პროკრედიტბანკის" ოფიციალურ უსაფრთხო ვებ–გვერდზე იმყოფებით, შეადარეთ უსაფრთხო კავშირის სიმბოლო.

Internet Explorer 9

ბოქლომზე დაჭერით ვებ–გვერდის უსაფრთხოების იდენტიფიცირების სერტიფიკატი გაიხსნება.

Internet Explorer 8



ბოქლომზე დაჭერით ვებ–გვერდის უსაფრთხოების იდენტიფიცირების სერტიფიკატი გაიხსნება.

Firefox 4

თქვენ გაქვთ საშუალება შეამოწმოთ "პროკრედიტ ბანკის" უსაფრთხოების სერტიფიკატი ბრაუზერში არსებულ “ბოქლომის” ნიშანზე დაწკაპუნებით.

მოერიდეთ თაღლითურ pop-up ფანჯრებს

მთლიანად გაყალბებული ვებ–გვერდის გახსნის სანაცვლოდ, თაღლითებს შეუძლიათ ჩატვირთონ ნამდვილი ვებ–გვერდი ბრაუზერის მთავარ ფანჯარაში და შემდეგ მასზე განათავსონ "pop-up" ფანჯარა. თუ გვერდი ამრიგად გაიხსნება, ნამდვილი ვებ–გვერდის სამისამართო ველი ვებ–გვერდის ფონზე გამოჩნდება, თუმცა "pop-up" ფანჯარაში თქვენს მიერ შეყვანილი ნებისმიერი ინფორმაცია თაღლითების ხელში ჩავარდება, რომლებიც მას საკუთარი მიზნებისთვის გამოიყენებენ.

ინტერნეტ ბანკინგის ანგარიშში შესასვლელად, ახალ ფანჯარაში მისამართი თავად აკრიფეთ. ინტერნეტ ბანკინგის ნამდვილი ვებ–გვერდის მისამართი დაიწყება ასოებით "https", ხოლო ბრაუზერის ფანჯრის ზედა ნაწილში პატარა ბოქლომი გამოჩნდება.