უსაფრთხო ინტერნეტ შოპინგი

ინტერნეტი გვთავაზობს შოპინგის კომფორტულ და მოსახერხებელ გზას. ნებისმიერ ადამიანს სახლიდან გაუსვლელად შეუძლია დაათვალიეროს, აარჩიოს მრავალი ინტერნეტ მაღაზიის მილიონობით პროდუქტი და განახორციელოს ონლაინ შესყიდვა.

მეორე მხრივ ინტერნეტ შოპინგი მიმზიდველია კიბერ-კრიმინალებისთვის, ვინაიდან არსებობს მრავალი მეთოდი, რომელთა გამოყენებითაც შესაძლებელია გაუთვიცნობიერებელი მომხმარებლის პერსონალური და ფინანსური ინფორმაციის მოპოვება. აღნიშნული ინფორმაციის ხელში ჩაგდების შემდეგ, კიბერ დამნაშავეს შეუძლია საკუთარი ფინანსური მიზნებით გამოიყენოს სხვისი კუთვნილი თანხა, სხვადასხვა ინტერნეტ მაღაზიაში.

ინტერნეტ შოპინგის ნებისმიერ ეტაპზე საჭიროა უსაფრთხოების ზომების მიღება და სათანადო ყურადღების გამოჩენა.

არსებობს ინტერნეტ შემსყიდველებზე კიბერ შეტევის ძირითადი სამი გზა:

- დაუცველ კომპიუტერებზე მოქმედება - თუ კომპიუტერის მომხმარებელი არ გაატარებს სათანადო ღონისძიებებს კომპიუტერის დასაცავად, ვირუსული და მავნე ფაილებისაგან, კიბერ შემტევებს შეუძლიათ მოიპოვონ წვდომა კომპიუტერში არსებულ ნებისმიერ ინფორმაციაზე.

- ცრუ საიტების და ელექტრონული ფოსტის შექმნა - შესაძლებელია ლეგალური ინტერნეტ მაღაზიების ზუსტი ასლის შექმნა მავნე, დამაინფიცირებელი შიგთავსით ან ელ-ფოსტის გაგზავნა ლეგალური ინტერნეტ მაღაზიის სახელით. თუ მომხმარებელი შეცდომაში შევიდა და გახსნა აღნიშნული ცრუ ინტერნეტ საიტი ან ელ-ფოსტა, მაშინ შესაძლებელია პერსონალური და ფინანსური მონაცემების ხელში ჩაგდება, შემტევების მიერ.

- არასაიმედოდ დაცული ტრანზაქციებში ჩარევა - თუ კომუნიკაციის არხი ინტერნეტ მაღაზიასა და მომხმარებელს შორის არ არის სათანადოდ დაცული

უსაფრთხოების პროტოკოლებით, მაშინ შესაძლებელია მესამე პირი ჩაერიოს ინფორმაციის ნაკადში და სრულად მოიპოვოს გადაცემული ინფორმაცია.

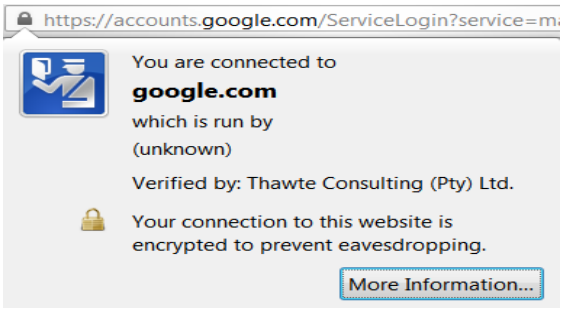
თავდაცვის მეთოდები და საშუალებები:

- Antivirus, Firewall, Anti-Spyware გამოყენება და გამართვა - ამ პროგრამების გამოყენებით შესაძლებელია კომპიუტერის დაცვა არასასურველი მავნე პროგრამებისაგან. ასევე საჭიროა ანტივირუსის ბაზების რეგულარულად განახლება.

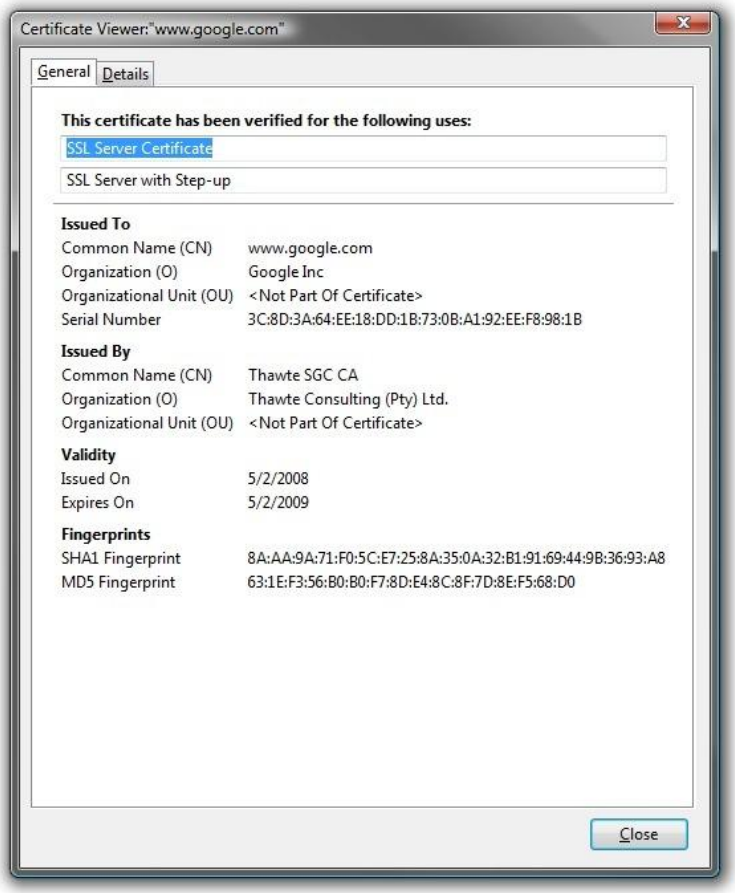
- კომპიუტერში არსებული პროგრამული უზრუნველყოფის, განსაკუთრებით ვებ ბრაუზერის განახლებების მუდმივი მონიტორინგი და ინსტალაცია. ბევრ ოპერაციულ სისტემას და კონკრეტულ პროგრამებს გააჩნია ავტომატური განახლების ფუნქცია (automatic updates). შედეგად კიბერ შემტევებს ინფორმაციის ხელში ჩაგდების ნაკლები შანსი ეძლევა, ვინაიდან პროგრამის განახლებები, ასწორებს ძველ ვერსიაში არსებულ სისუსტეებს.

- პროგრამების პარამეტრების შეფასება - მრავალი პროგრამის საწყისი პარამეტრები (Default Setting) არ არის დაკონფიგურირებული უსაფრთხოების მოთხოვნების შესაბამისად. სასურველია ყოველი ასეთი პარამეტრის შემოწმება და მაქსიმალური უსაფრთხოების დონის გამოყენება, რაც კიდევ უფრო მეტ დაცვას შესძენს კომპიუტერს ინტერნეტში მუშაობისას.

- შოპინგისათვის მაღალი რეპუტაციის და სანდო ინტერნეტ საიტების გამოყენება. კიბერ-დამნაშავეები ქმნიან რეალური საიტის ცრუ ანალოგებს. საჭიროა ასევე ვებ-საიტის უსაფრთხოების სერტიფიკატის შემოწმება, რათა დავრწმუნდეთ რომ საქმე გვაქვს რეალურ ლეგალურ საიტთან. ბრაუზერის მისამართის ველში უნდა ეწეროს HTTPS და შემდგომ ინტერნეტ მისამართი: მაგალითები სხვადასხვა ბრაუზერის მიხედვით:

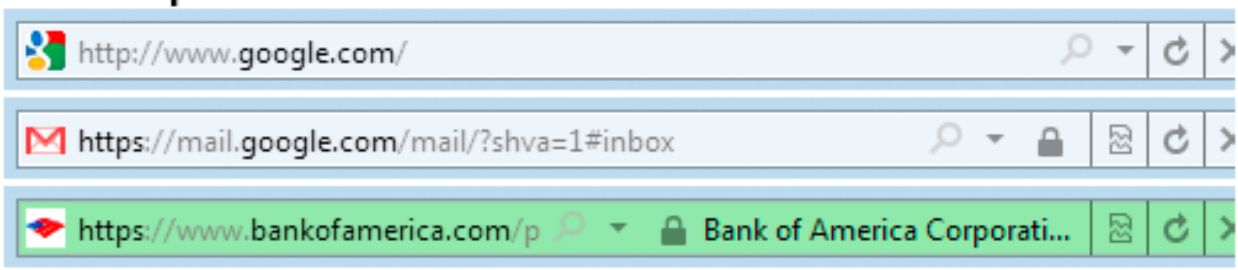


კომპანია google-ის მიერ გაცემული ლეგალური სერტიფიკატი

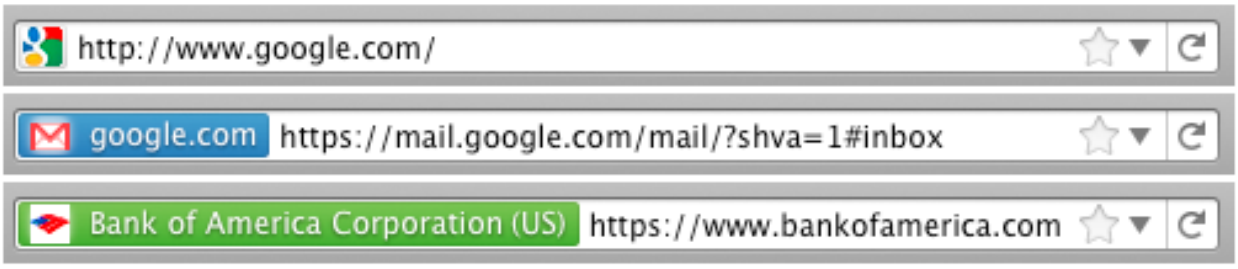


სხვადასხვა ინტერნეტ ბრაუზერებში შოპინგის დროს დაცული კავშირი გამოსახულია 2-3 სამისამართე ველებში:

Internet Explorer 9

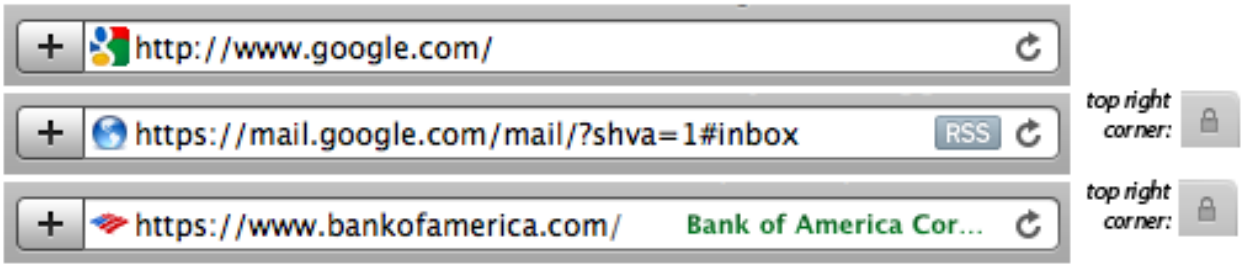


Firefox 4



Chrome 8

Safari 4



- რთული პაროლის გამოყენება. საჭიროა ინტერნეტ მაღაზიაში რეგისტრაციისას მაქსიმალურად რთული პაროლის გამოყენება (საიდუმლო სიტყვა უნდა

შეიცავდეს ციფრებს, დიდ და პატარა ასოებს, სპეციალურ სიმბოლოებს). მარტივი პაროლი: pass1234, iloveyou, windows777 და ა.შ. რთული პაროლი: H8akN#$al2.

- სიფრთხილის გამოჩენაა საჭირო მიღებული ელექტრონული ფოსტის გახსნისას. კიბერ-დამნაშავეები გზავნიან ცრუ ელ-ფოსტას ინტერნეტ მაღაზიების სახელით, და მომხმარებელი შეყავთ შეცდომაში, ითხოვენ მათგან გარკვეულ ინფორმაციას, პაროლის შეცვლას, საკრედიტო ბარათების კოდების დადასტურებას და ა.შ.

- თავის დაცვის მიზნით არ უნდა გადაიგზავნოს ელ-ფოსტით პერსონალური მონაცემები, ასევე წერილში აღნიშნულ საიტებზე და ლინკებზე შესვლა განსაკუთრებით სახიფათოა.

- სანამ რომელიმე ორგანიზაციას ანდობთ პრივატულ, პერსონალურ და საფინანსო ინფორმაციას რეკომენდირებულია მათი „Privacy Policy“ გაცნობა. ამ დოკუმენტში განხილული იქნება, თუ როგორ შეინახავს და გამოიყენებს ორგანიზაცია, თქვენს მიერ მინდობილ პერსონალურ ინფორმაციას.

- საკრედიტო ბარათების მუდმივი მონიტორინგი, ამონაწერის და გადარიცხვების ისტორიის თვალყურის დევნება. შესაბამისად ნებისმიერი საეჭვო ტრანზაქციის შემთხვევაში, ბარათის და ანგარიშის დროებითი ბლოკირებით დაიცავთ თავს ფინანსური ზარალისგან.