ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი

ინტერნეტ უსაფრთხოების 10 წესი

საკონტაქტო ინფორმაცია:

ალ.გრიბოედოვის ქ.
№3 საქართველო, 0180,
თბილისი
ტელ: + 995 32 2 92 15 14
ელ-ფოსტა: info@idfi.ge
ვებ-გვერდი: www.idfi.ge

**ოქტომბერი,
2017**

შინაარსი

1. შექმენით საიმედო პაროლი

პაროლი - თქვენი მონაცემების დაცვის ყველაზე მარტივი საშუალებაა. მის შერჩევას სიფრთხილით მიუდექით. მოერიდეთ მარტივი ციფრებისა და ასოების კომბინაციას, განსაკუთრებით, თუ იგი თქვენივე პირად მონაცემებს შეიცავს.

როგორ შევქმნა საიმედო პაროლი?

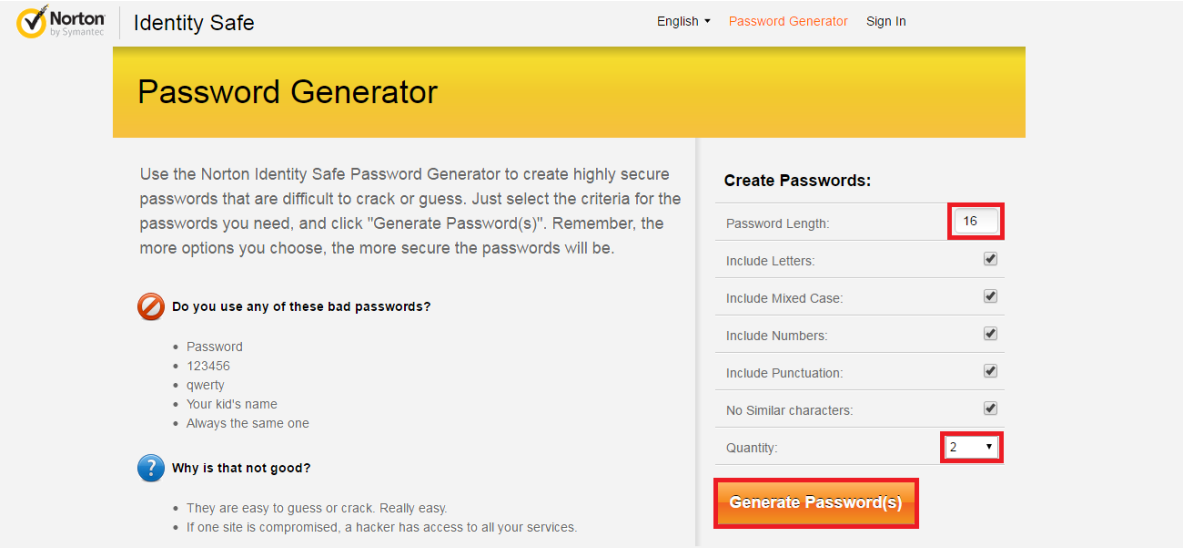
მრავალფეროვნება - მოერიდეთ მოკლე სიტყვების და მარტივი ციფრების კომბინაციას. გამოიყენეთ დიდი და პატარა ასოები, სასვენი ნიშნები, ციფრები და სხვა სიმბოლოები.
სიგრძე - სასურველია, პაროლი მინიმუმ 16 სიმბოლოსგან შედგებოდეს. ხრიკი: მოიფიქრეთ მარტივი წინადადება, რომელსაც შემდეგ გაართულებთ მრავალფეროვანი სიმბოლოებით (მაგ: msopliossauketesoparoli à Ms0pl1os,S@uk3tesO-parol!).

როგორ გამოვიყენო პაროლი უსაფრთხოდ?

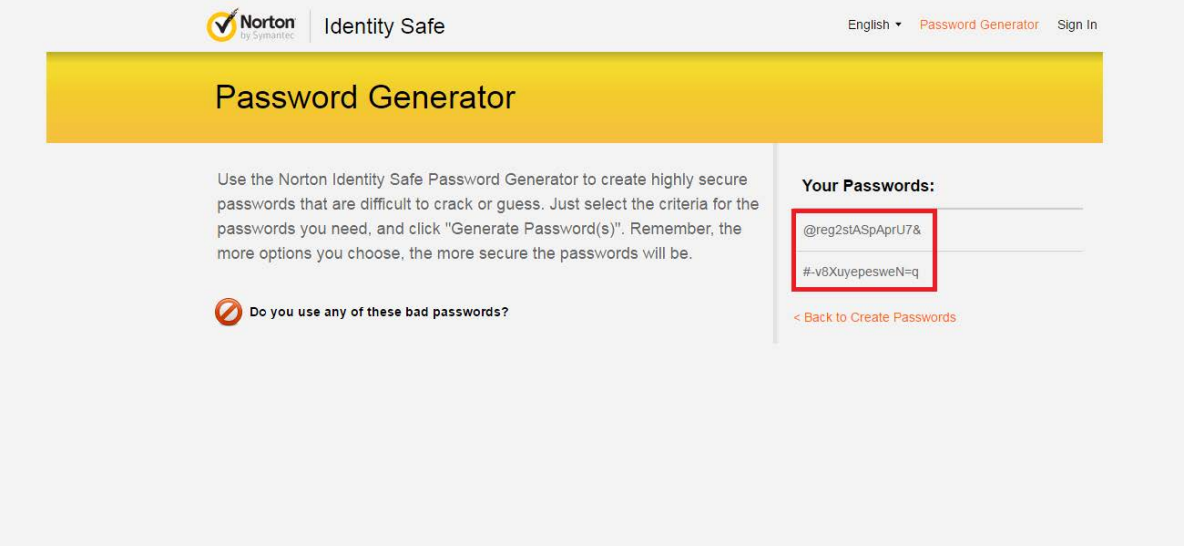
განახლება - ხშირად შეცვალეთ პაროლები (მაგალითად, სამ თვეში ერთხელ).
პირადი ინფორმაცია - ნუ გამოიყენებთ თქვენს პირად ინფორმაციას (შვილის სახელი ან საცხოვრებელი მისამართი...) პაროლად.
გაზიარება - არ გაუზიაროთ პაროლი გარეშე პირებს.
საერთო სივრცე - მოერიდეთ პაროლების შეყვანას საერთო მოხმარების კომპიუტერებში და ისეთ ადგილებში, სადაც კამერებია დაყენებული.
გამეორება - ნუ გამოიყენებთ ერთსა და იმავე პაროლს სხვადასხვა ანგარიშისთვის და ვებგვერდისთვის.

დამხმარე საშუალებები

იმისათვის, რომ პაროლი საიმედო იყოს, საჭირო არაა იგი თავად მოიფიქროთ. უმჯობესია, გამოიყენოთ ონლაინ სერვისები, რომლებიც რთულად გასაშიფრი პაროლის გენერირებას ახდენენ. ამგვარი სერვისია მაგალითად Identity Safe, რომელიც პაროლს შემთხვევითობის პრინციპით, სასურველი სიმბოლოების სახეობებითა და სირთულით არჩევს.



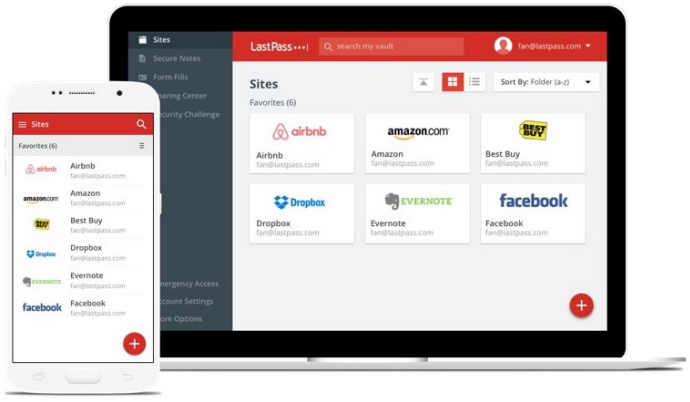
სურათი 1: *როგორ ვისარგებლო Identity Safe სერვისით: აირჩიეთ სასურველ პაროლში არსებული სიმბოლოების რაოდენობა და თუ რამდენი პაროლის შექმნა გსურთ. შემდეგ კი, აირჩიეთ „გენერირება“*



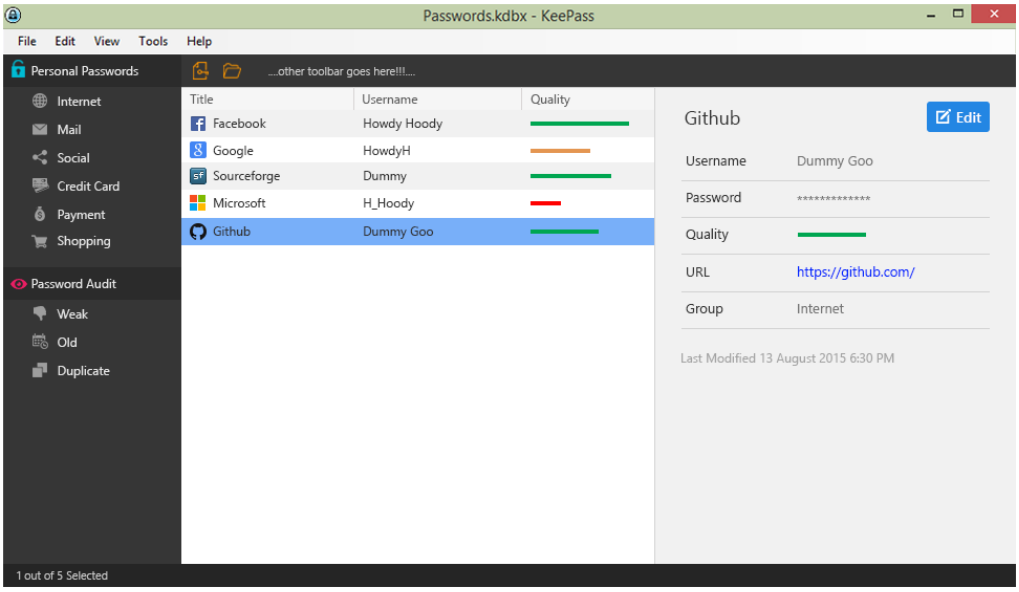
სურათი 2: *შექმნილი პაროლები ეკრანის ზედა მარჯვენა კუთხეში გამოჩნდება*

პაროლების შემნახველი აპლიკაციები

რთული და დიდი რაოდენობის პაროლების დასამახსოვრებლად არსებობს პაროლის შემნახველი სერვისები, მაგალითად როგორიცაა, LastPass ან KeepPass. მათ ასევე რთული პაროლების შექმნის ფუნქციაც აქვთ. დააყენეთ აპლიკაცია თქვენს ელექტრონულ მოწყობილობაში და ერთ სივრცეში მოუყარეთ თავი სხვადასხვა გვერდისთვის შექმნილ პაროლებს.



სურათი 3: *რთული პაროლების დასამახსოვრებლად გამოიყენეთ აპლიკაცია LastPass -* www.lastpass.com



სურათი 4: *რთული პაროლების დასამახსოვრებლად ასევე შეგიძლიათ, გამოიყენოთ აპლიკაცია KeepPass - www.keepass.info*

ხშირად შეცვალეთ პაროლები და დამატებითი უსაფრთხოებისათვის, არ შეიყვანოთ ისინი საზოგადოებრივი თავშეყრის იმ ადგილებში, სადაც კამერებია დაყენებული. ასევე ნუ გამოიყენებთ ერთსა და იმავე პაროლს სხვადასხვა აპლიკაციასა და ვებგვერდისათვის.

2. დაშიფრეთ თქვენი მონაცემები

ინფორმაციის დაშიფვრა შეგიძლიათ მყარ დისკსა და ინფორმაციის შემნახველზე (ოპტიკური დისკები, USB flash drive და ა.შ.). თუ კომპიუტერი და მისი მყარი დისკი უცხო ადამიანთა ხელში აღმოჩნდა, სპეციალური პაროლის შეყვანის გარეშე ვერ შეძლებენ დისკზე არსებული ინფორმაციის გახსნას. შესაბამისად, დისკზე შენახული ყველა ინფორმაცია მათთვის გაუგებარი დარჩება.

როგორ დავშიფრო ინფორმაცია?

Apple-ის კომპიუტერებზე (OS X): გამოიყენეთ FileVault პროგრამა, რომელსაც მთლიანი დისკის დაშიფვრის ფუნქცია აქვს. იგი Mac OS X-ს ავტომატურად მოჰყვება, შესაბამისად, თქვენ არ დაგჭირდებათ მისი გადმოწერა და დაყენება.

სურათი 5: *როგორ გავააქტიურო FileVault პროგრამა: ეწვიეთ თქვენი მოწყობილობის უსაფრთხოების პარამეტრებს და აირჩიეთ „FileVault“, შემდეგ კი - „Turn on FileVault“. მომავალში ცვლილებების თავიდან ასარიდებლად, ასევე მონიშნეთ ეკრანის მარცხენა ქვედა კუთხეში გამოსახული სიმბოლო*

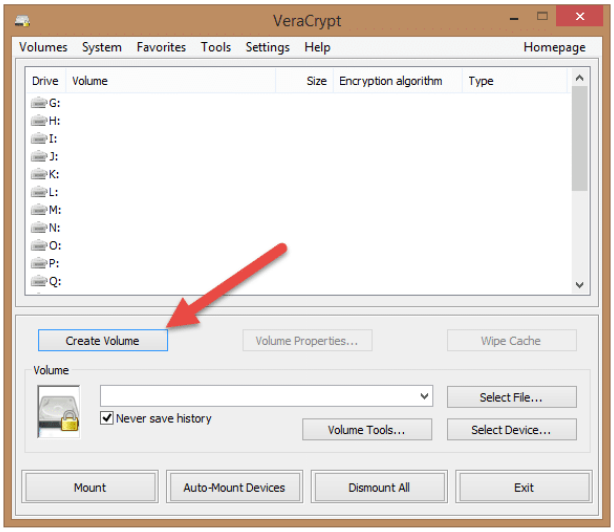
სურათი 6: *მონიშნეთ თითოეული მომხმარებელი, ვის ანგარიშზეც გსურთ ფუნქციის გააქტიურება*

სურათი 7: *შეინახეთ ან დაიმახსოვრეთ აღმდგენი გასაღები, რომელიც პაროლის დავიწყების შემთხვევაში გამოგადგებათ*

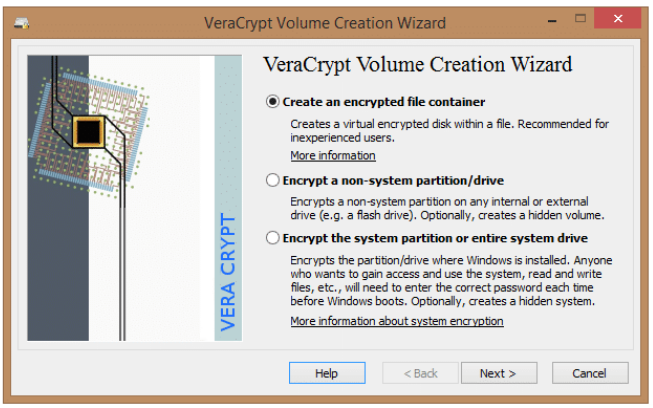
სურათი 8: *თუკი აღმდგენ გასაღებს დაკარგავთ, თქვენ შეძლებთ, დაუკავშირდეთ Apple-ს მის დასაბრუნებლად. ამისათვის საჭიროა, უპასუხოთ მითითებულ სათადარიგო შეკითხვებს*

სურათი 9: *თქვენი მოწყობილობის გადატვირთვასთან ერთად, სისტემა ავტომატურად დაიწყებს მყარი დისკის დაშიფვრას*

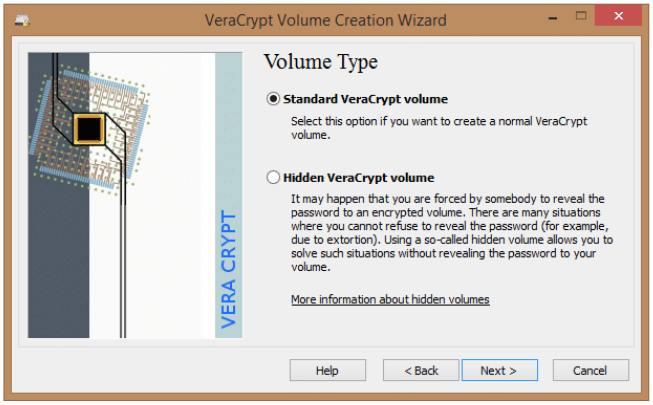
Windows OS კომპიუტერებზე: Microsoft-ის ოპერაციული სისტემების პროფესიონალურ ვერსიებს (Enterprise, Pro, Ultimate Edition) ჩაშენებული აქვთ პროგრამა BitLocker (მყარი დისკის სრულად დაშიფვრის ფუნქცია). სხვა დანარჩენი შემთხვევებისთვის არსებობს პროგრამა VeraCrypt.



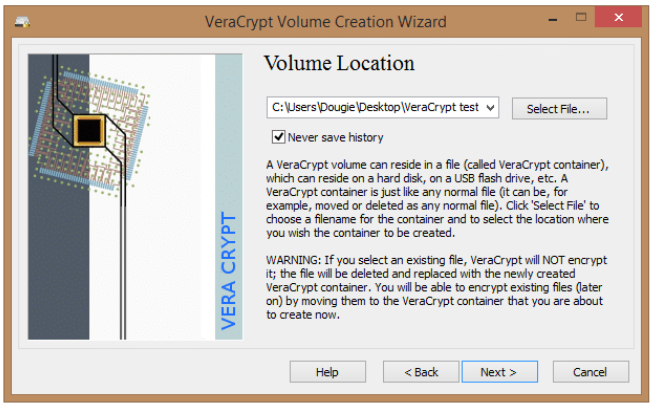
სურათი 9: *როგორ ვისარგებლო პროგრამა VeraCrypt-ით: გადმოწერეთ და დააყენეთ VeraCrypt თქვენს მოწყობილობაზე, შემდეგ კი მთავარ ეკრანზე მონიშნეთ "Create Volume"*



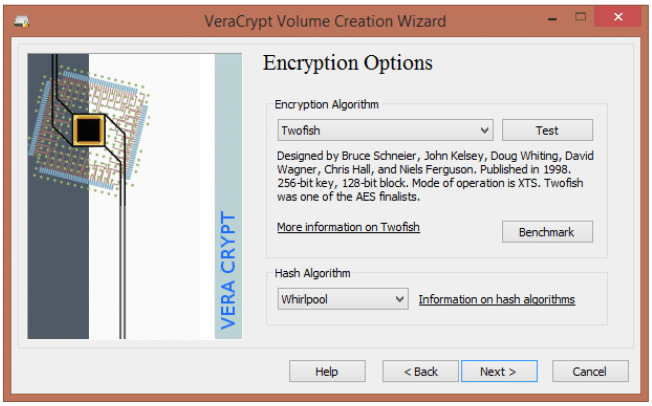
სურათი 10: *მონიშნეთ "Standard VeraCrypt volume"*



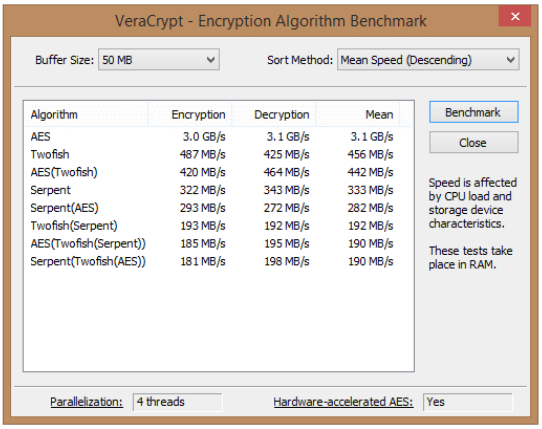
სურათი 11: *მიუთითეთ, თუ სად გსურთ ფაილის შენახვა*



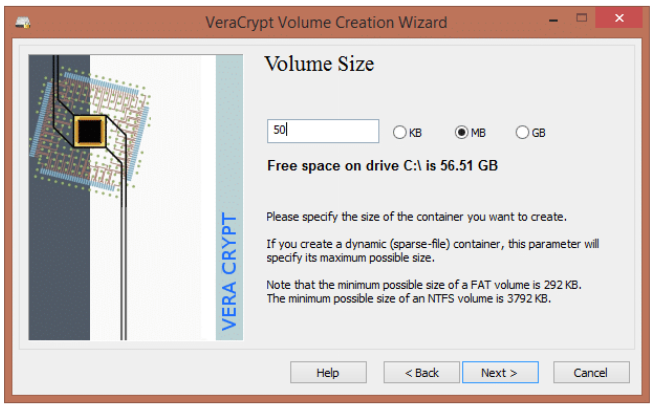
სურათი 12: *მიუთითეთ, თუ სად გსურთ ფაილის შენახვა*



სურათი 13: *მიუთითეთ დაშიფვრის ალგორითმი (თითოეულ ალგორითმს თან ახლავს მის შესახებ ინფორმაცია, რაც გეხმარებათ, შეარჩიოთ თქვენთვის ყველაზე სასურველი დაშიფვრის მეთოდი)*

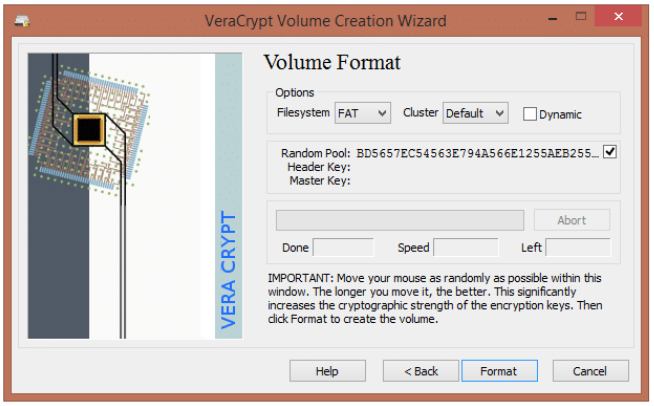


სურათი 14: *შეგიძლიათ, შეამოწმოთ, რამდენად სწრაფად მუშაობს დაშიფვრის თითოეული მეთოდი*



სურათი 15: *ასევე შეგიძლიათ, აირჩიოთ შესანახი ფაილის მოცულობა*

სურათი 16: *აირჩიეთ პაროლი*



სურათი 17: *მოცულობის ფორმატის არჩევის შემდეგ, თქვენ დაასრულებთ დაშიფრული ფაილების საცავის შექმნის პროცესს*

3. დაშიფრეთ ელ-ფოსტა

ელექტრონული ფოსტა კომუნიკაციის ერთ-ერთ ყველაზე პოპულარულ მეთოდს წარმოადგენს, რომელიც როგორც საქმიანი, ასევე პირადი მიმოწერისათვის გამოიყენება. მაგრამ ხშირად იგი „ფიშინგის“ (ინტერნეტ-თაღლითობის სახეობა, რომელიც მიზნად ისახავს პირადი მონაცემების ხელში ჩაგდებას) სამიზნე ხდება. პირადი მიმოწერის სხვის ხელში ჩაგდებისგან თავის ასაცილებლად აუცილებელია ელ-ფოსტის დაშიფვრა.

ელექტრონული ფოსტის დასაშიფრად გამოიყენეთ PGP ტექნოლოგია (Pretty Good Privacy). ის შეტყობინებას გაგზავნამდე შიფრავს და მხოლოდ სპეციალური პაროლის მქონე პირებს შეუძლიათ მისი შინაარსის წაკითხვა.

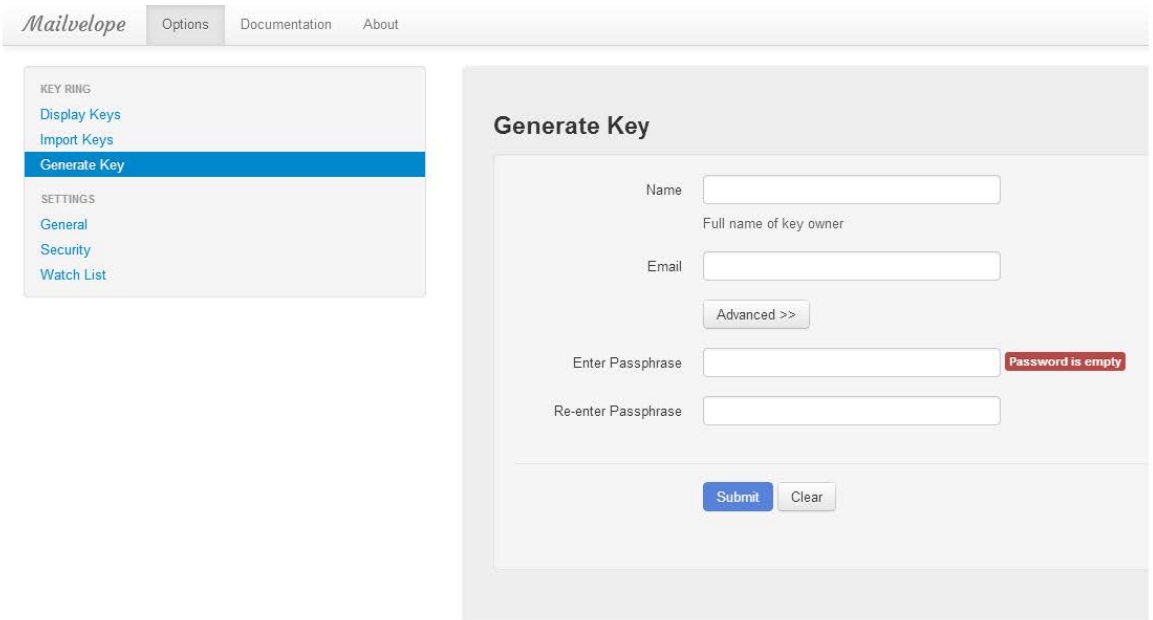
იმ შემთხვევაშიც კი, თუკი თქვენი წერილი სხვის ხელში აღმოჩნდება, მისი შინაარსი უცნობი დარჩება.

როგორ მუშაობს PGP?

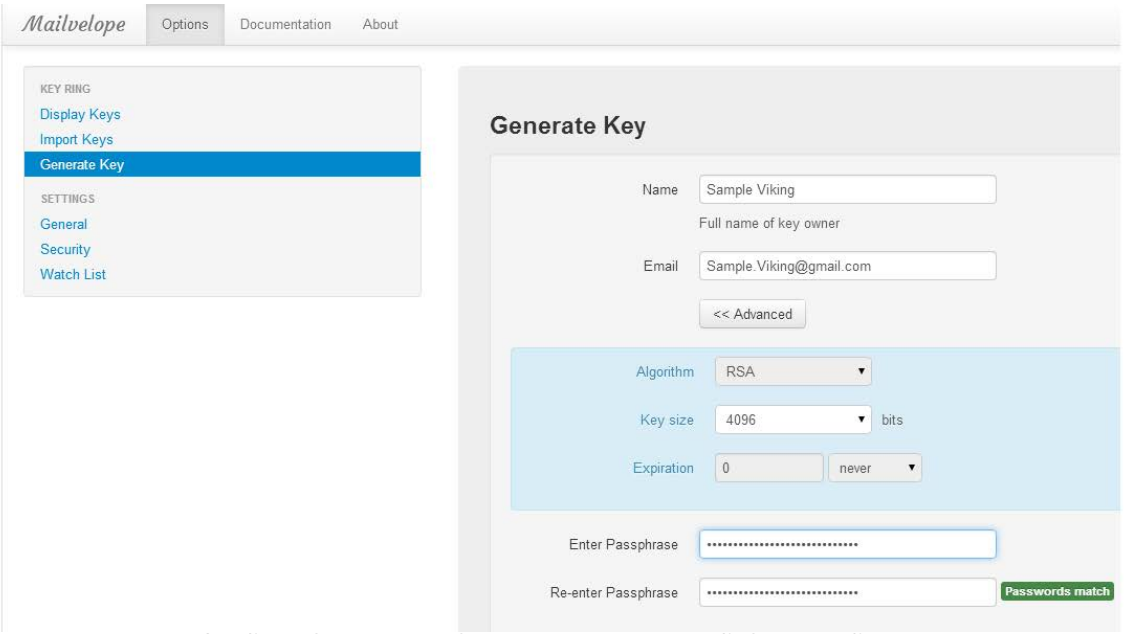
თქვენს კომპიუტერზე დაყენებული სპეციალური პროგრამის მეშვეობით (მაგ: MailVelope ბრაუზერებისათვის და Enigmail ელ-ფოსტისათვის) თქვენი საფოსტო ყუთისათვის ქმნით ღია და დახურულ გასაღებებს, ასევე წერილების დასაშიფრად საჭირო მძლავრ პაროლს. როდესაც გსურთ, ვინმეს დაშიფრული წერილი გაუგზავნოთ, პირველ რიგში ერთმანეთში უნდა გაცვალოთ ღია გასაღებები. თქვენი მოსაუბრის ღია გასაღები კი, უნდა შეიყვანოთ თქვენივე გასაღებების სიაში. ამის შემდეგ, უნდა შეხვიდეთ საკუთარ საფოსტო ყუთში რომელზეც PGP ტექნოლოგიაა გააქტიურებული:
აკრიფოთ შეტყობინების ტექსტი
მიუთითოთ ადრესატი
დაყენებული პროგრამის მეშვეობით დაშიფროთ ტექსტი (თქვენი და ადრესატის ღია გასაღებების გამოყენებით)
გაგზავნეთ შეტყობინება

ხოლო თუ ვერ ახერხებთ მნიშვნელოვანი წერილის დაშიფრვას, მაშინ მისი შიგთავსი მოათავსეთ ფაილში, დაშიფრეთ ფაილი, მიაბით წერილს და ისე გაგზავნეთ.
თუ თქვენ დაშიფრულ წერილს მიიღებთ, მის გასაშიფრად დაგჭირდებათ შეიყვანოთ პაროლი, რომელსაც საფოსტო ყუთი წერილის გახსნისას მოგთხოვთ.

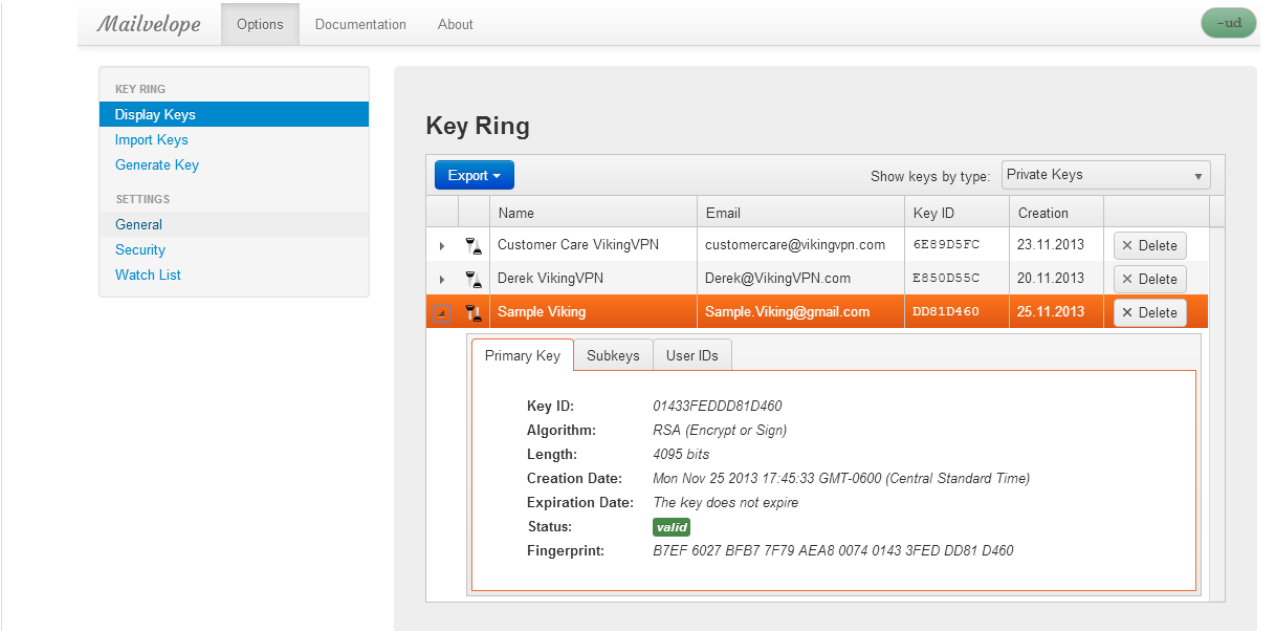
ქვემოთ მოცემულია თუ როგორ მუშაობს დაშიფვრის აღნიშნული საშუალება (PGP) MailVelope პროგრამის მაგალითზე, რომელიც Chrome-ისა და Firefox-ის ვებ ბრაუზერში გაფართოების სახით (extension) შეიძლება დაყენდეს.



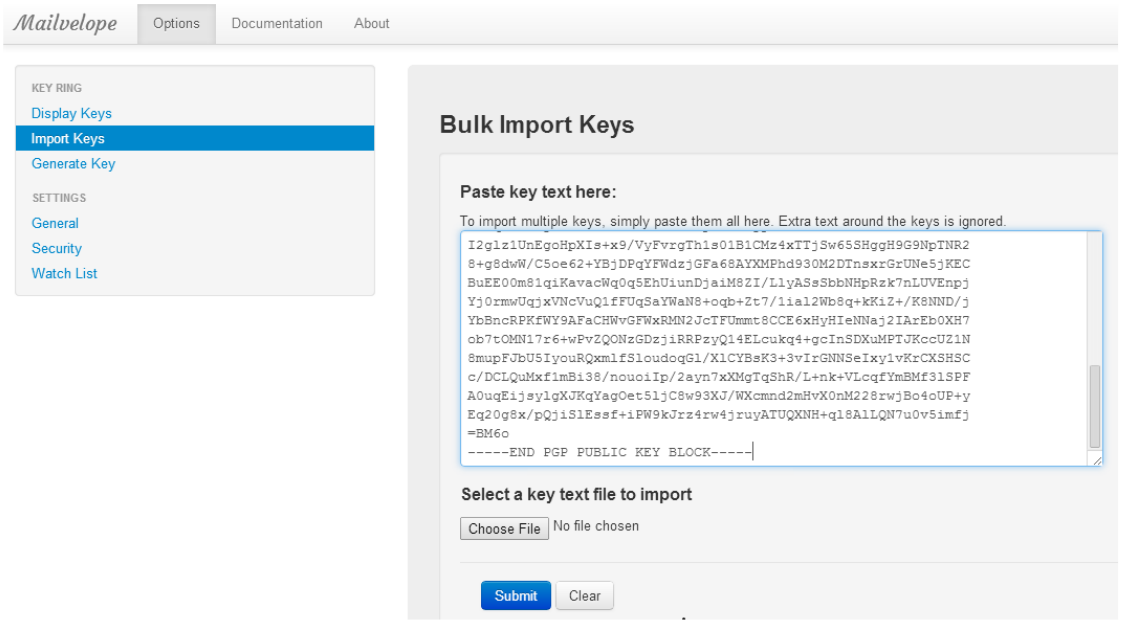
სურათი 18: *როგორ ვისარგებლო PGP ტექნოლოგიით, MailVelope პროგრამის შემთხვევაში: იგი Chrome-ისა და Firefox-ის ვებბრაუზერში გაფართოების სახით (extension) შეიძლება დაყენდეს*



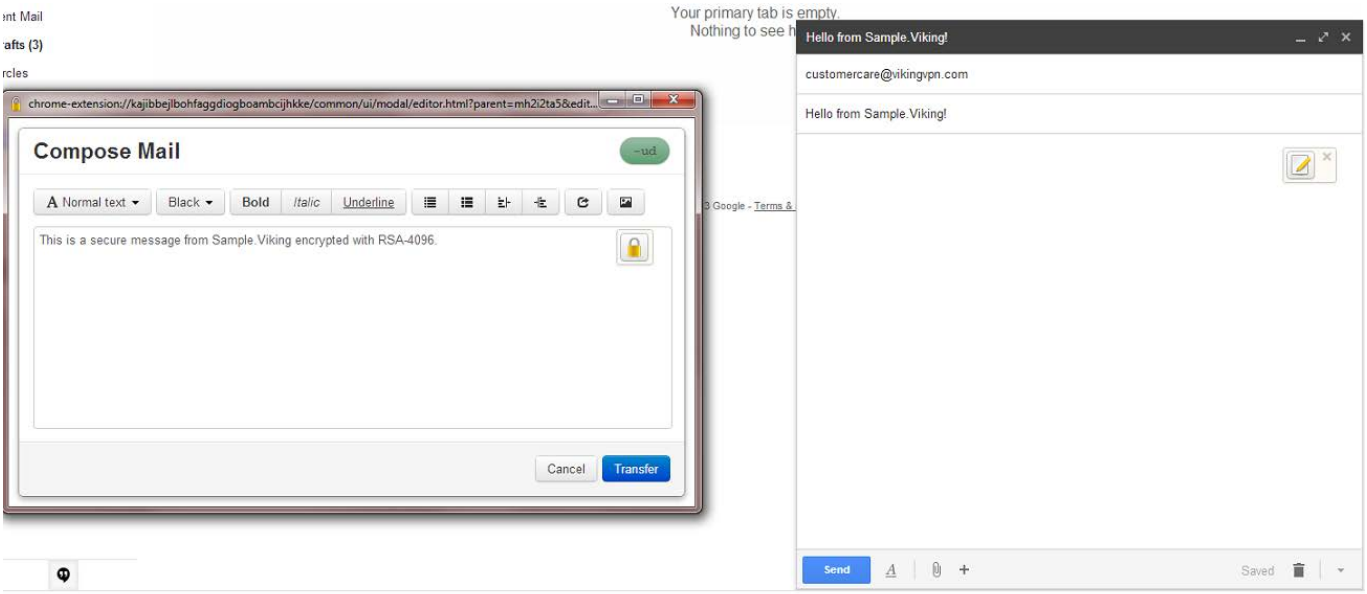
სურათი 19: *ახალი გასაღების შესაქმნელად აირჩიეთ "Generate Key", შემდეგ კი, შეიყვანეთ თქვენი მონაცემები. ასევე შეარჩიეთ პაროლი და სასურველი დაშიფვრის ალგორითმი*



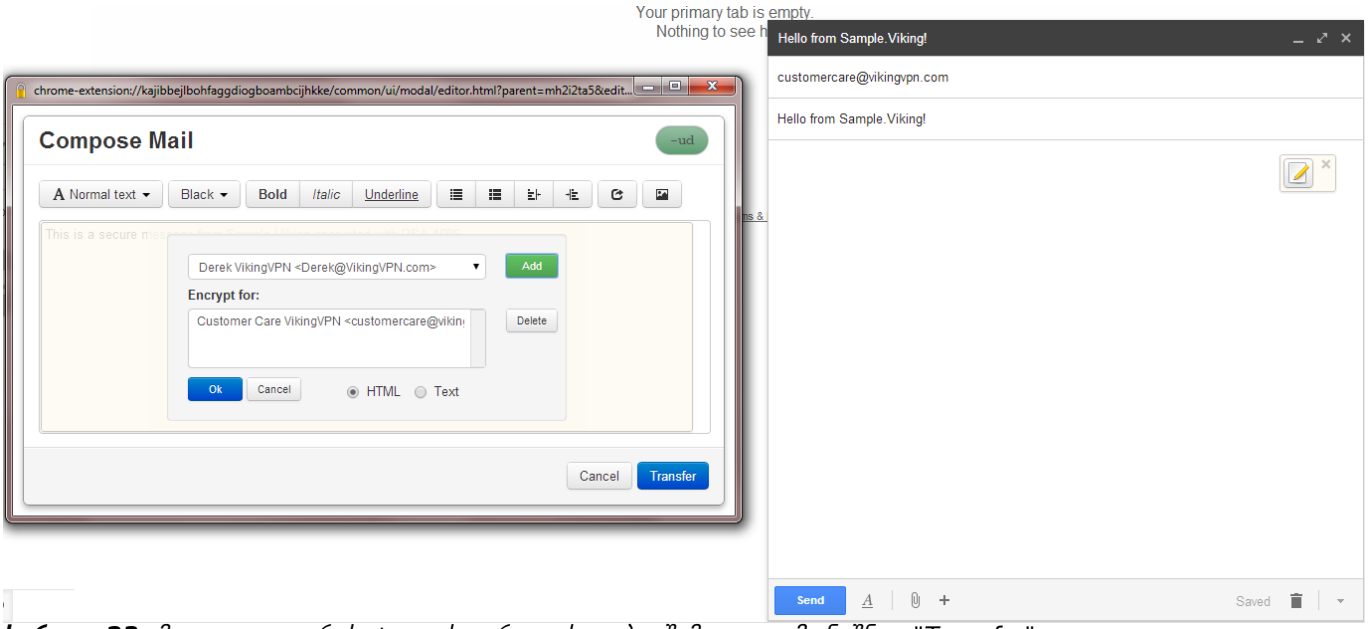
სურათი 20: *აირჩიეთ "Display Keys" და ეკრანზე გამოჩნდება თქვენი გასაღებები, მათი შექმნის დრო, ვადის გასვლის თარიღი და ა.შ. ამ ჩამონათვალში მონიშნეთ თქვენს მიერ ახლადშექმნილი გასაღები და დააჭირეთ "Export" -ს. ამ შემთხვევაში მიიღებთ საჯარო გასაღებს, რომელიც ნებისმიერ იმ ადამიანს უნდა გაუზიაროთ, ვისგანაც დაშიფრული წერილის მიღება გსურთ*



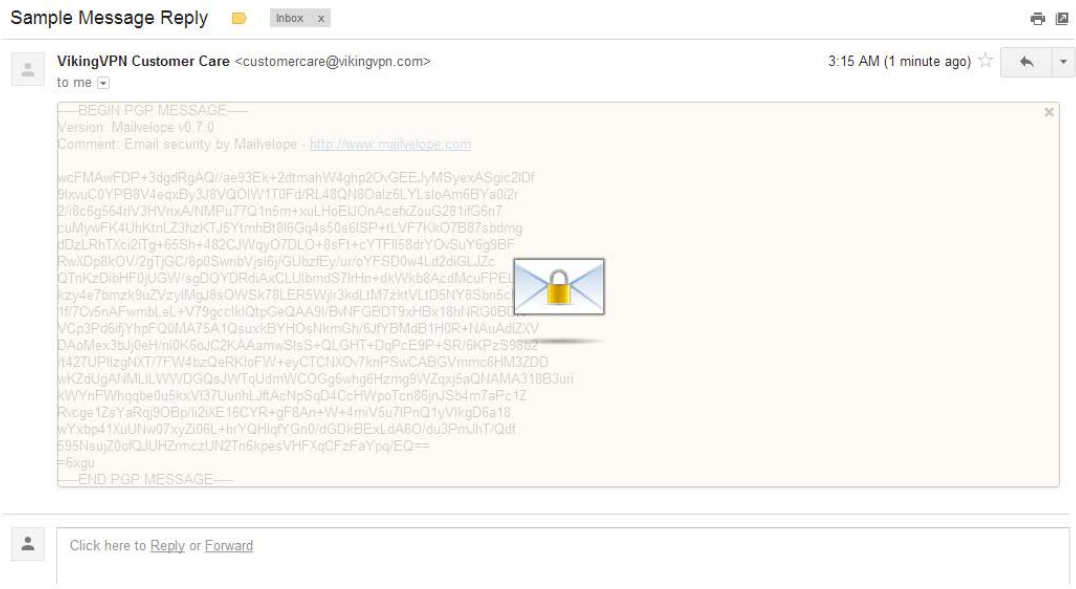
სურათი 21: *მონიშნეთ "Import Keys" და სისტემაში შეინახეთ გასაღები, რომელსაც იმ პირისგან მიიღებთ, ვისთანაც დაშიფრული წერილის გაგზავნა გსურთ*



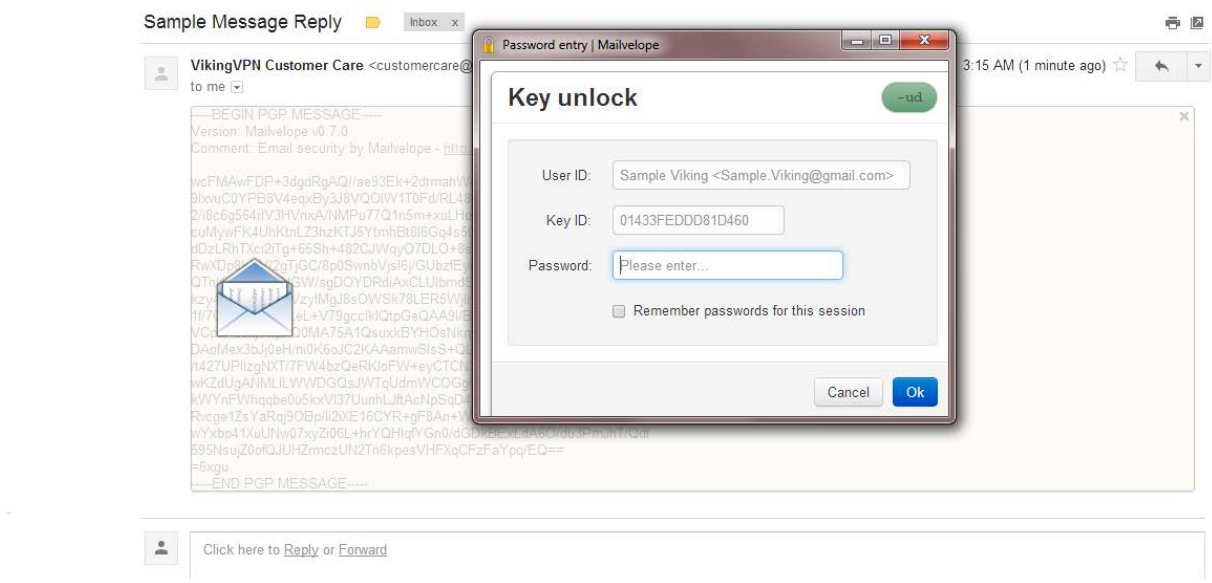
სურათი 22: *წერილის გაგზავნამდე უნდა მონიშნოთ ეკრანზე ნაჩვენები კლიტე*



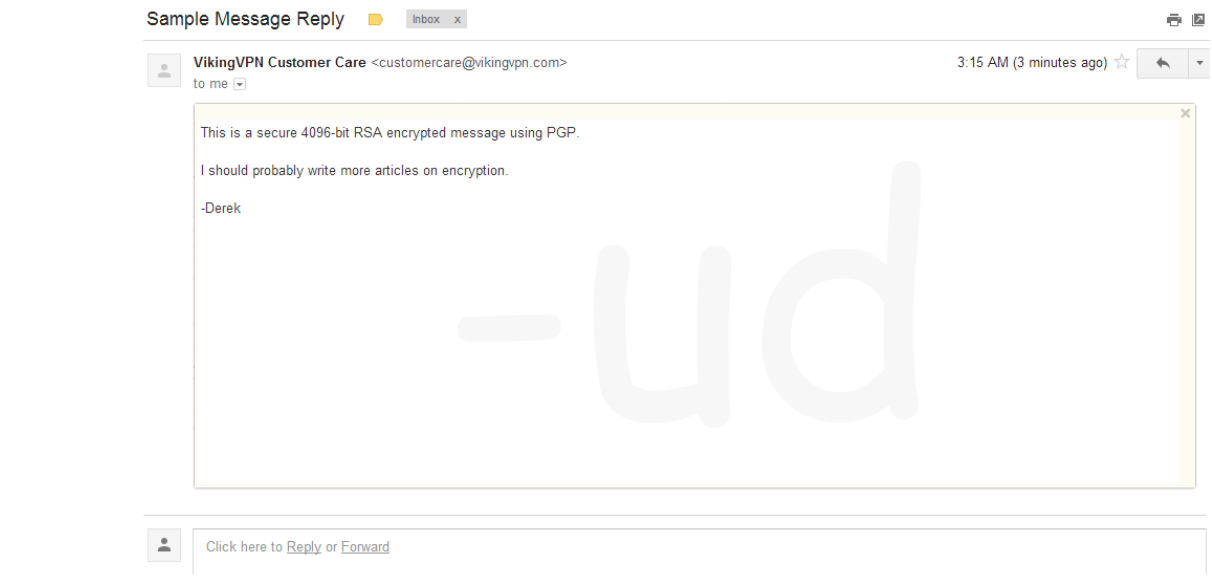
სურათი 23: *მიუთითეთ ადრესატი და საჯარო გასაღები. შემდეგ კი, მონიშნეთ "Transfer"*



სურათი 24: *დაშიფრული შეტყობინების წასაკითხათ კი, პაროლის შეყვანა დაგჭირდებათ*



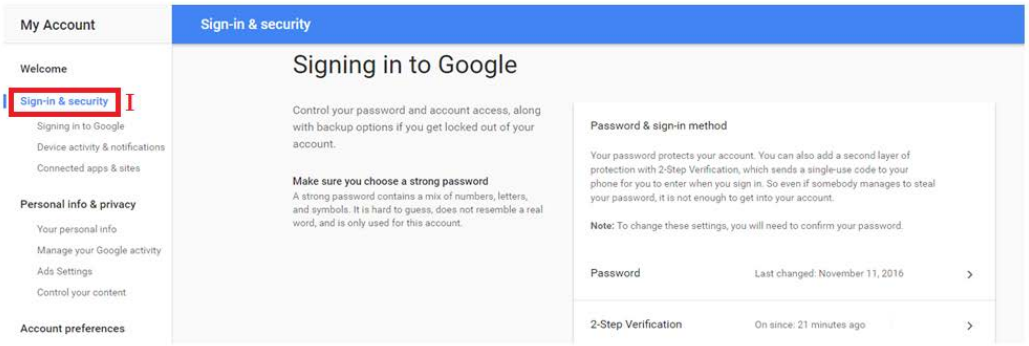
სურათი 25: *შეიყვანეთ პაროლი*



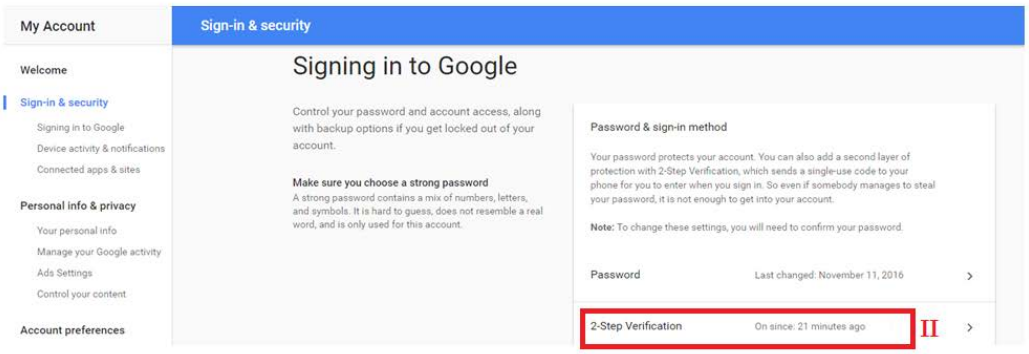
სურათი 26: *პაროლის შეყვანის შემდეგ თქვენ შეძლებთ დაშიფრული შეტყობინების წაკითხვას*

4. დააყენეთ ანგარიშზე არაავტორიზებული შესვლისგან დამცავი დამატებითი საშუალება

არაავტორიზებული შესვლისგან თავის დასაცავად, სადაც შესაძლებელია, ჩართეთ ორფაქტორიანი ავტორიზაცია. ეს არის დამატებითი დაცვის საშუალება სოციალურ ქსელებში, მესენჯერებში, ელფოსტაზე, Google-ში და ა.შ. ამ ფუნქციის ჩართვის შემთხვევაში, თქვენს ანგარიშზე შესასვლელად პაროლთან ერთად ერთჯერადი კოდის შეყვანაც მოგიწევთ. კოდს SMS-ის საშუალებით მიიღებთ. ასევე, თუ ტელეფონზე დაყენებული გაქვთ პაროლების გენერატორი აპლიკაცია, კოდს ამ პროგრამიდან მიიღებთ.



სურათი 27: *როგორ გავააქტიუროთ ფუნქცია Google-ის ანგარიშზე შესასვლელად: გადადით თქვენი ანგარიშის პარამეტრებში, შემდეგ კი, მონიშნეთ "Sign-in & security"*



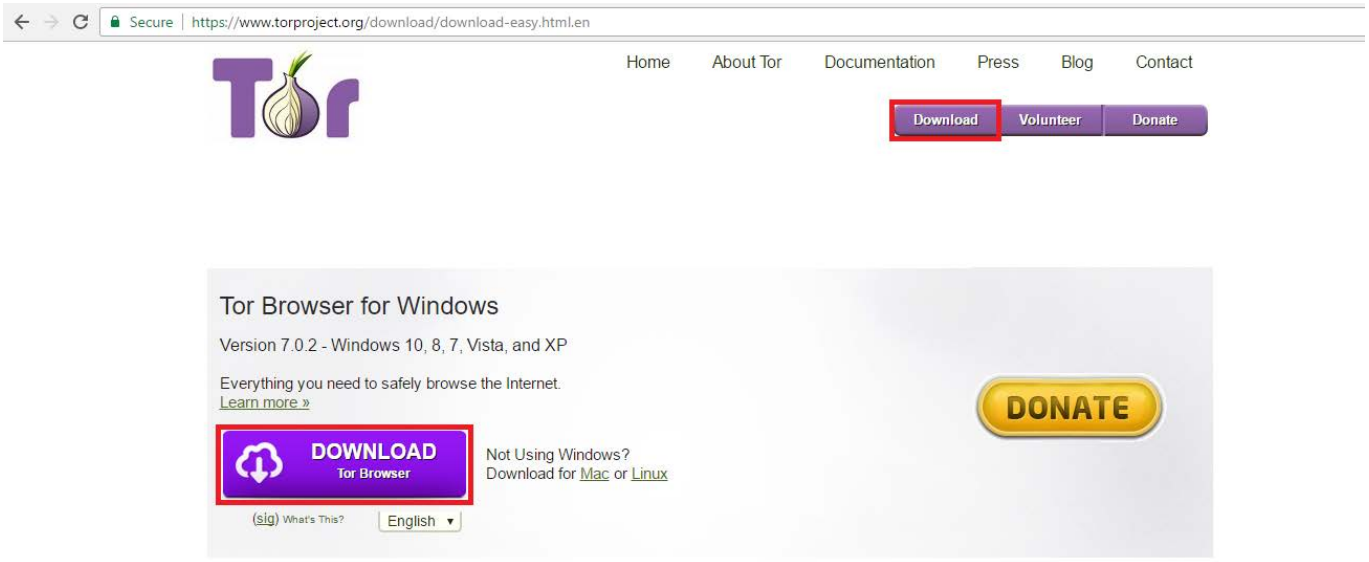
სურათი 28: *გააქტიურეთ "2-Step Verification" ველი*

5. დაიცავით ანონიმურობა ქსელში

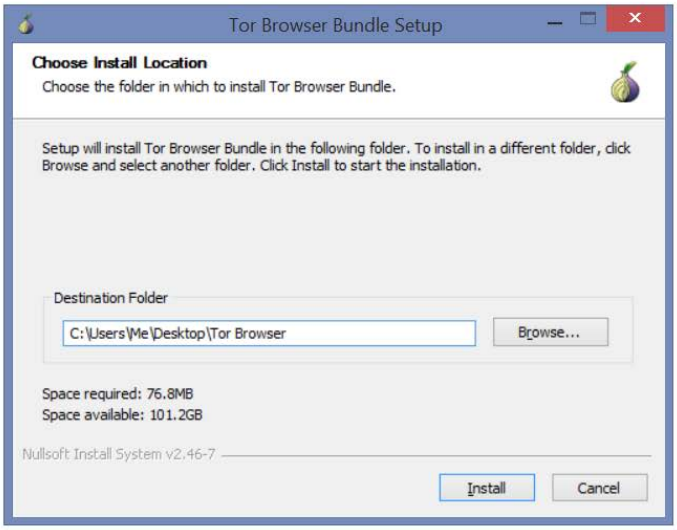
ქსელში ანონიმურობის დასაცავად გამოიყენეთ VPN (Virtual Private Network - ვირტუალური პირადი ქსელი). ეს ტექნოლოგია საშუალებას გაძლევთ, თუნდაც უცხო ქვეყნიდან, ისარგებლოთ ინტერნეტ რესურსებით ისე, რომ ვერავინ შეძლოს თქვენი ადგილსამყოფელის დადგენა. VPN მომსახურებას VPN პროვაიდერები უზრუნველყოფენ. გაითვალისწინეთ, რომ ასეთ მომსახურებას ორი მთავარი მახასიათებელი ჰქონდეს: ის არ უნდა ინახავდეს თქვენს მონაცემებს და უნდა გააჩნდეს გარე სერვერები, რათა შეძლოთ, აირჩიოთ, თუ რომელი ქვეყნიდან გსურთ დაფიქსირდეთ ამა თუ იმ ვებგვერდზე შესვლისას.

ინტერნეტში თქვენი ნაკვალევის დაფარვის კიდევ ერთი საშუალებაა Tor Browser. Tor-ით სარგებლობისას, ვერ მოხერხდება თქვენს ინტერნეტ აქტივობაზე თვალის მიდევნება, შესაბამისად დაინტერესებული პირებისათვის უცნობი დარჩება, თუ რომელ ვებგვერდებს სტუმრობთ; ასევე იმ ვებგვერდებისათვის, რომლებსაც თქვენ სტუმრობთ უცნობი დარჩება თქვენი ადგილსამყოფელი, რადგან თქვენი ინტერნეტ ტრაფიკი სხვადასხვა Tor სერვერებზე ნაწილდება. მისი მეშვეობით, დაბლოკილ საიტებზეც გექნებათ წვდომა.

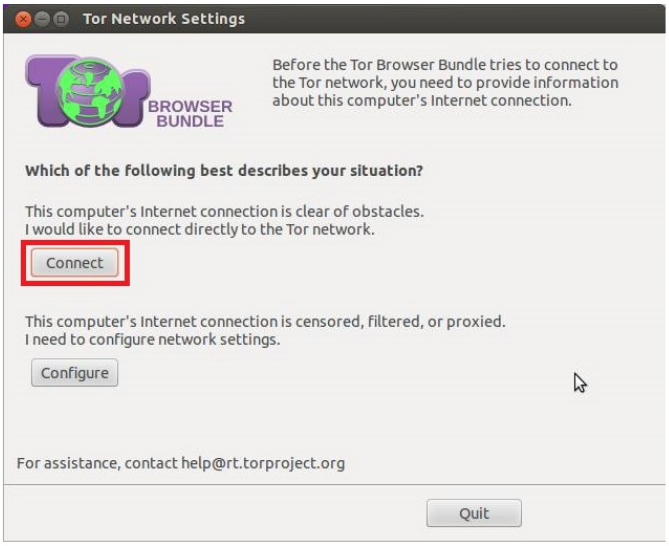
Tor გამორჩეულად პოპულარულია ჟურნალისტებს და აქტივისტებს შორის, რომლებიც იმ ქვეყნებში მუშაობენ, სადაც ხშირია ინტერნეტ შეზღუდვები. Tor-ის გამოყენება როგორც Windows-ის, ასევე MacOS-ისა და Linux-ის მომხმარებლებისთვისაა შესაძლებელი.



სურათი 29: *როგორ გამოვიყენო Tor Browser: გადმოწერეთ და დააყენეთ იგი თქვენს მოწყობლობაში (ამისათვის ეწვიეთ www.torproject.org). Tor Browser იმ ბრაუზერების (Chrome, Firefox და ა.შ) ნაცვლად უნდა გამოიყენოთ, რომლებითაც ჩვეულებრივ სარგებლობთ. Tor თავისთავად Firefox-ის სახეცვლილი ვერსიაა*

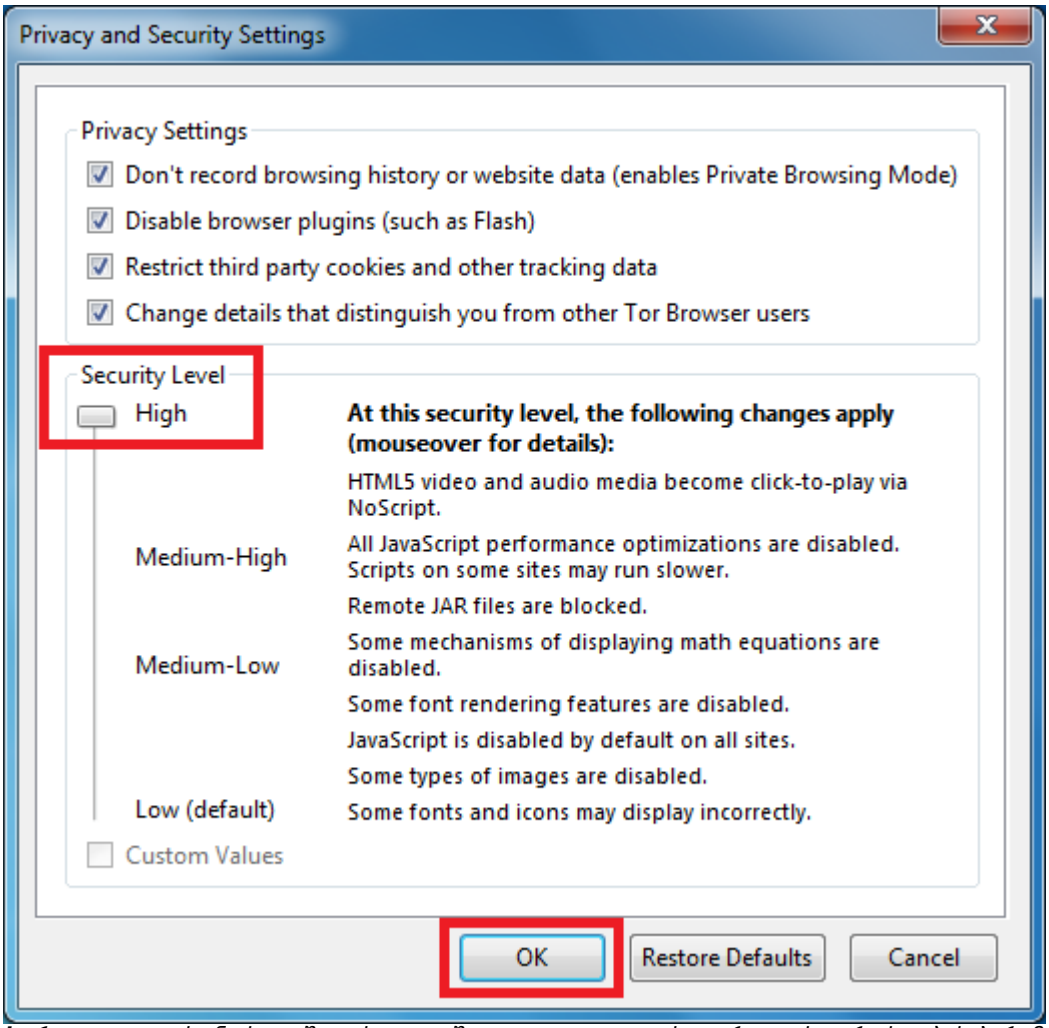


სურათი 30: *Tor პორტატული პროგრამაა (რაც ნიშნავს რომ მისი გამოყენება ნებისმიერი ადგილიდან, მაგალითად USB მოწყობილობიდანაცაა შესაძლებელი) და იგი ჩვეულებრივი პროგრამების მსგავსად არ ინსტალირდება. Tor ავტომატურად თქვენს სამუშაო მაგიდას აირჩევს სასურველ ლოკაციად. თუ ლოკაციის შეცვლა გსურთ, აირჩიეთ "Browse", შემდეგ კი ადგილმდებარეობა*

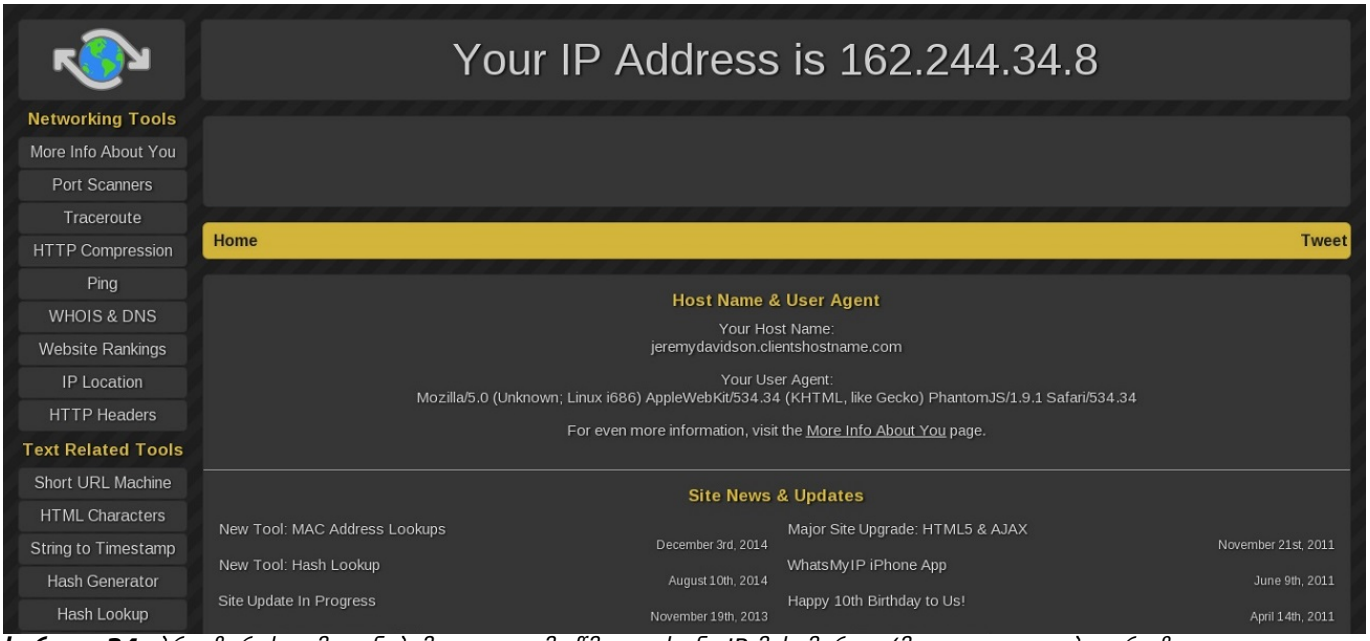


სურათი 31: *თუკი ქსელზე ცენზურა ან მონიტორინგი ხორციელდება, ან ის გარკვეულწილად შეზღუდულია, ბრაუზერის კონფიგურაცია დაგჭირდებათ. ამისათვის აირჩიეთ "Configure", სხვა დანარჩენ შემთხვევაში კი, "Connect"*

სურათი 32: *ქსელთან დაკავშირებამ შესაძლოა რამდენიმე წუთი წაგართვათ, შემდეგ კი, თავისუფლად შეძლებთ ბრაუზერით სარგებლობას*



სურათი 33: *თქვენ ასევე შეგიძლიათ, შეცვალოთ და გააძლიეროთ უსაფრთხოების პარამეტრები. ამისათვის მონიშნეთ ბრაუზერის მარცხენა კუთხეში არსებული სიმბოლო; უსაფრთხოების დონის მისათითებლად კი გამოიყენეთ სლაიდერი*



სურათი 34: *ბრაუზერის გამოყენებამდე გადაამოწმეთ თქვენი IP მისამართი (მაგალითად ვებგვერდზე whatsmyip.org), თუ შემოწმებისას თქვენი ნამდვილი მისამართი არ გამოჩნდება, ე.ი თქვენ სწორად მოიხმართ ბრაუზერს*

როგორ მოვიქცეთ თუ ვებგვერდი დაგვიბლოკეს?

თუ თქვენს ქვეყანაში კონკრეტული ვებგვერდი დაიბლოკება, არსებობს გზები აღიდგინოთ მასზე წვდომა. Chrome-ის ან Firefox-ის მოხმარების შემთხვევაში დააინსტალირეთ Frigate ან Zenmate. მათი დახმარებით, თქვენ თითქოს სხვა ქვეყნიდან სტუმრობთ დაბლოკილ ვებგვერდებს.

დაბლოკილ ვებგვერდებზე წვდომაში ასევე დაგეხმარებათ Proxfree. ეწვიეთ საიტს და მიუთითეთ სასურველი მისამართი.

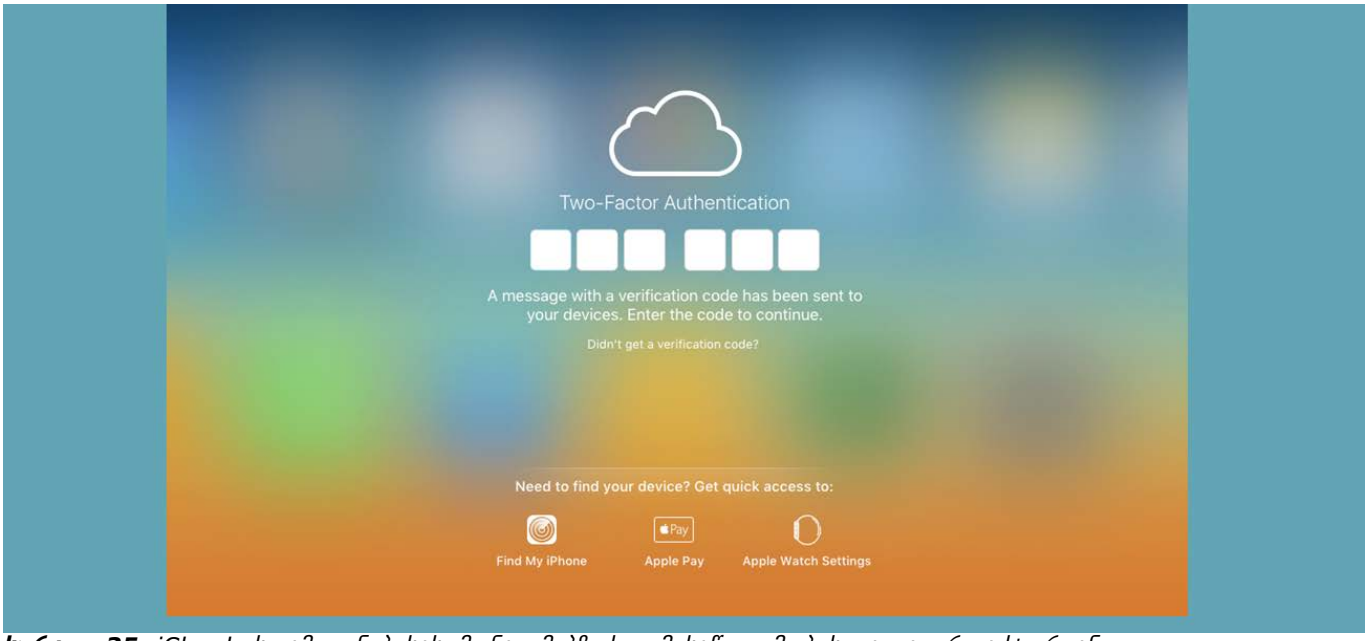
თუ თქვენ სარგებლობთ IPHONE-ით ან IPAD-ით, გადმოწერეთ ბრაუზერი Onion. ის 1$ ღირს და მისი მეშვეობით დაბლოკილ ვებგვერდებთან გექნებათ წვდომა. ასევე არსებობს Zenmate iOS-ისთვის.

თუ თქვენ Android სმართფონით სარგებლობთ, Play Market-ზე შეგიძლიათ იპოვნოთ უფასო ბრაუზერი Orfox, რომელიც Onion ბრაუზერის ანალოგიურია. ასევე არსებობს Zenmate Android-ისთვის.

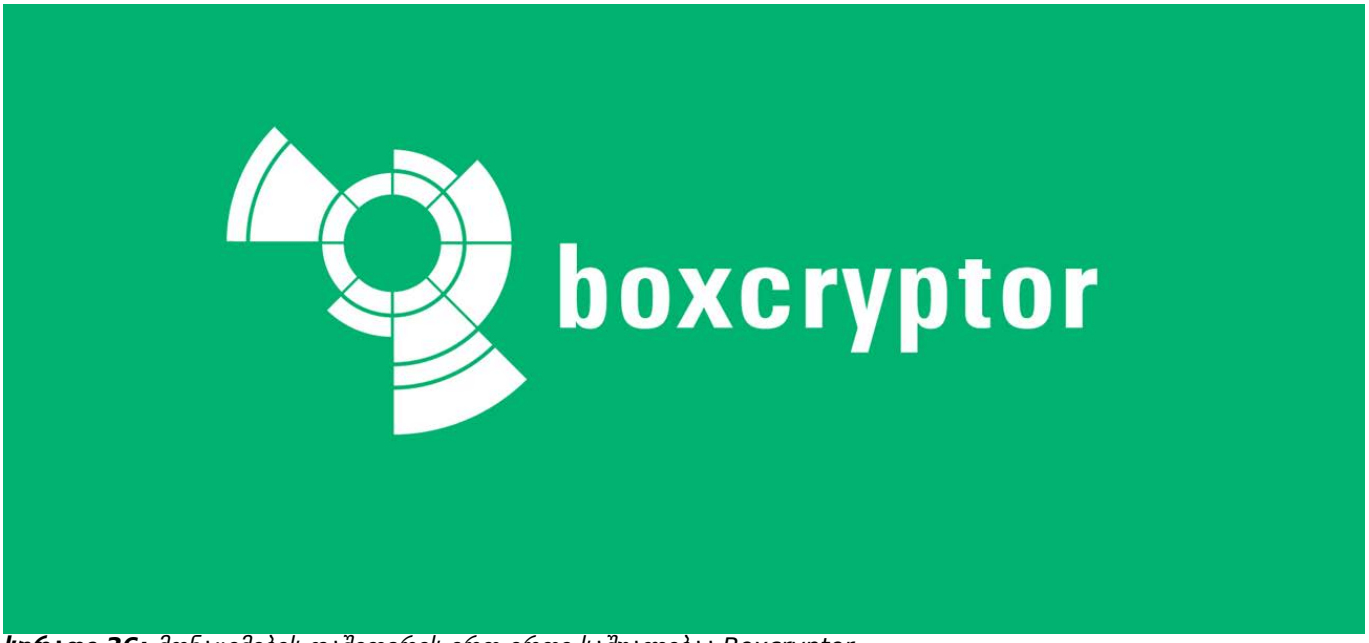
6. გამოიყენეთ სარეზერვო მონაცემების საცავი

თუ რომელიმე მოწყობილობა დაგეკარგათ, ეს არ ნიშნავს, რომ მასში დაცული ინფორმაციაც სრულად დაკარგეთ.
Google Drive საცავი დაკავშირებულია თქვენს Google ანგარიშთან. მასზე შეგიძლიათ დააყენეთ ორფაქტორიანი ავტორიზაცია, ნახოთ თქვენ მიერ დათვალიერებული ვებგვერდების სია (browsing history) და ჩართოთ გაფრთხილების შეტყობინება, რომელიც მოგივათ იმ შემთხვევაში, თუ თქვენს ანგარიშზე უცნობი მოწყობილობიდან შევლენ. Google Drive თავად არ შიფრავს მონაცემებს. ამისთვის, საჭიროა გამოიყენოთ სხვა სერვისები, როგორებიცაა Boxcryptor ან VeraCrypt.

Apple-ის მომხმარებლები მონაცემების შესანახად iCloud-ის სერვისს იყენებენ. მასზე ხელმისაწვდომობის დაცვაც ორფაქტორიანი ავტორიზაციითაა შესაძლებელი. დაშიფრული მონაცემების ერთ-ერთი პოპულარული შემნახველია Mega. ის ინფორმაცია, რაც მის სერვერზე ინახება, თავად სერვისის ადმინისტრაციისთვისაც არ არის ხელმისაწვდომი. თქვენი ანგარიშის პაროლი უნიკალური გასაღებ-გამშიფრავია, თუმცა, გაითვალისწინეთ, რომ მისი დაკარგვა თქვენი ყველა მონაცემის წაშლას გამოიწვევს.

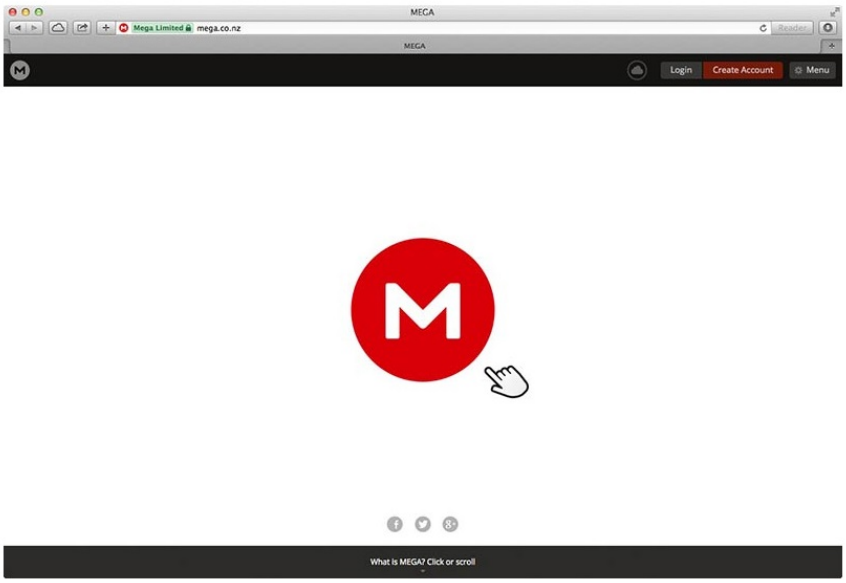


სურათი 35: *iCloud-ის გამოყენებისას, მონაცემებზე ხელმისაწვდომობის დაცვა ორფაქტორიანი ავტორიზაციითაა შესაძლებელი*



სურათი 36: *მონაცემების დაშიფვრის ერთ-ერთი საშუალებაა Boxcryptor*

სურათი 37: *დაშიფვრის ალტერნატიული საშუალებაა VeraCrypt*



სურათი 38: *თუ დაშიფრული მონაცემების შესანახად Mega-ს იყენებთ, დაიმახსოვრეთ, რომ თქვენი ანგარიშის პაროლი უნიკალური გასაღებ-გამშიფრავია. მისი დაკარგვა თქვენი ყველა მონაცემის წაშლას გამოიწვევს*

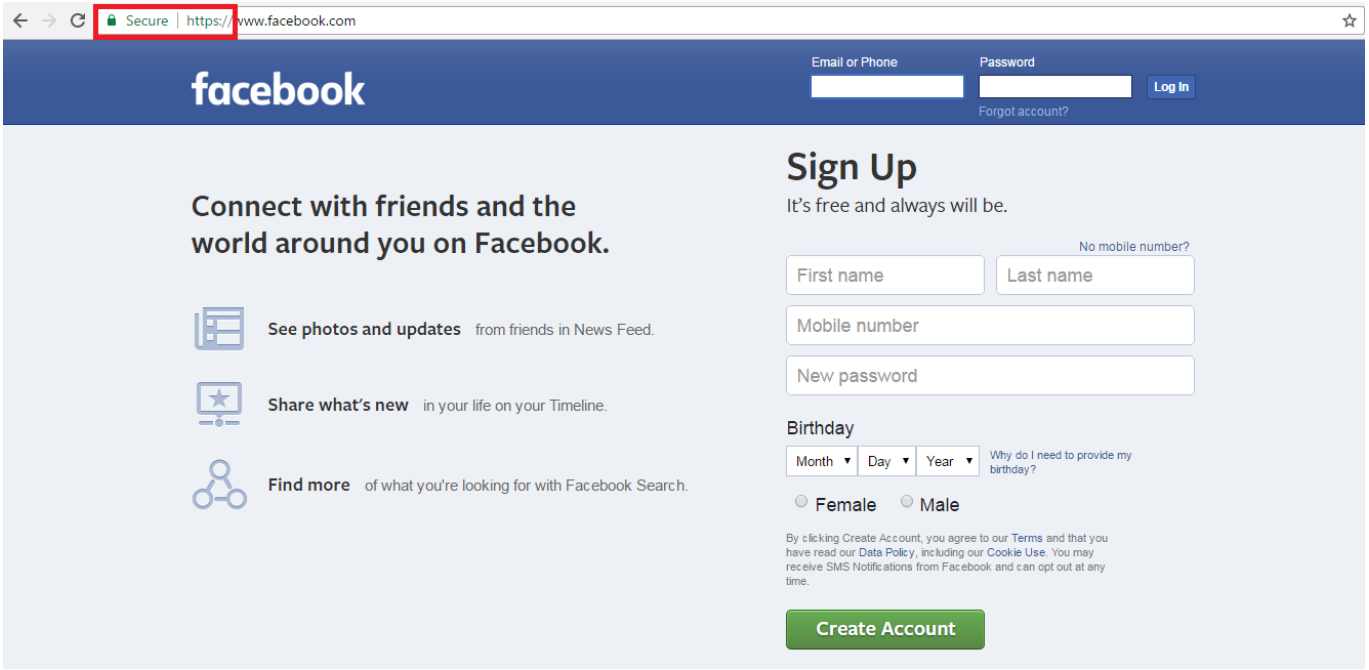
7. მნიშვნელოვანი ინფორმაცია მხოლოდ დაცულ ვებგვერდებზე შეიყვანეთ

ნებისმიერი ინფორმაცია: პაროლი, საბანკო ბარათის ნომერი და ა.შ, შეიყვანეთ მხოლოდ იმ ვებგვერდებზე, რომელსაც ჩართული აქვს HTTPS, ანუ ინფორმაციის დაშიფრული სახით გადაცემის მეთოდი. ის ჩვეულებრივი HTTP პროტოკოლისგან იმით განსხვავდება, რომ შიფრავს თქვენ მიერ შეყვანილ მონაცემებს, რის გამოც შეუძლებელია ისინი სხვის ხელში აღმოჩნდეს.

პირველ რიგში, დააკვირდით ბრაუზერში ვებგვერდის მისამართს. ხედავთ მწვანე ნიშანს და HTTPS აბრევიატურას? თუ არა, მაშინ თქვენი მოწყობილობიდან ვებგვერდზე მონაცემების შეყვანისას ისინი არ იშიფრება და შესაძლებელია მათი მითვისება.

ყოველთვის შეამოწმეთ, რამდენად უსაფრთხოა სისტემაში შესვლა (მომხმარებლის სახელით და პაროლით) და დააკვირდით სერვისის ვებმისამართი შეიცავს თუ არა „https://“-ს (სადაც „s“ აღნიშნავს უსაფრთხოს - „Secure”).

Google Chrome ავტომატურად ურთავს HTTPS ყველა იმ ვებგვერდს, რომელზეც ის უზრუნველყოფილია. ის მუშაობს როგორც უმრავლესობა ბანკების საიტებზე, ისე სოციალურ ქსელ Facebook-ზე:



სურათი 39

8. მინიმუმადე დაიყვანეთ თქვენი თვალთავლისა და მოსმენის შესაძლებლობა

დღესდღეობით, სპეციალური პროგრამების გამოყენებით, დაინტერესებულ პირებს თქვენი კომპიუტერის, ტელეფონის ან პლანშეტის კამერასა და მიკროფონთან დაკავშირება შეუძლიათ. დამატებითი უსაფრთხოების მიზნით, შეგიძლიათ დაფაროთ თქვენი ნოუთბუქის ვებკამერა. ვინაიდან, კომპიუტერის მიკროფონის ამოღება არ შეიძლება, მნიშვნელოვანი საუბრებისას მოწყობილობა გამორთეთ.

თუ თქვენი ადგილსამყოფელის გამჟღავნება არ გსურთ, სმარტ ტელეფონზე გამორთეთ გეოლოკაციის დამდგენი აპლიკაცია. ასევე, ტელეფონი გადაიყვანეთ „ფრენის რეჟიმზე“ (Airplane Mode).

9. დაიცავით უსაფრთხოება სოციალურ ქსელებში (Facebook)

Facebook-ის მოხმარებისას პირადი ინფორმაციის დასაცავად აუცილებელია რამდენიმე ძირითადი უსაფრთხოების წესის დაცვა. IDFI-მა სპეციალური გზამკვლევი შექმნა, სადაც შეგიძლიათ, გაეცნოთ ზოგად რჩევებს თუ როგორ აირიდოთ თავი უცხო ჯგუფებში გაწევრიანებისა და ანგარიშის გატეხვისგან, როგორ გადაამოწმოთ უსაფრთხოების პარამეტრები, აკონტროლოთ, თუ ვის შეუძლია თქვენი პოსტების ნახვა და თქვენი მონიშვნა სხვადასხვა პოსტებსა და ფოტოებზე.

გზამკვლევი ასევე ყურადღებას ამახვილებს პირადი მონაცემების მართვაზე. მისი გამოყენებით, გაიგებთ, თუ როგორ უნდა დააღწიოთ თავი ონლაინ რეკლამებს და დაიცვათ პირადი მიმოწერის უსაფრთხოება.

დეტალებისთვის იხილეთ გზამკვლევის სრული ვერსია.

10. დაიცავით ინფორმაციული „ჰიგიენის” ძირითადი წესები

უსაფრთხოების კონკრეტული პროგრამების და საშუალებების გარდა, არსებობს რამდენიმე მარტივი წესი, რომლის გამოყენებაც მინიმუმამდე ამცირებს როგორც მოწყობილობების, ისე ანგარიშის გატეხვისა და პირადი ინფორმაციის გაჟონვის რისკებს:

უსაფრთხო კომპიუტერის გამოყენება - მნიშვნელოვანი ოპერაციების შესასრულებლად (მაგ: ფინანსური გადარიცხვები, ბილეთების შეძენა და ა.შ) აუცილებლად გამოიყენეთ უსაფრთხო კომპიუტერი. უმჯობესია არ გამოიყენოთ სხვისი, საერთო ან უცნობი მოწყობილობები. გახსოვდეთ, რომ კომპიუტერი, რომლითაც სამსახურში სარგებლობთ, არა თქვენ, არამედ თქვენს დამსაქმებელს ეკუთვნის და შესაძლოა პიროვნებამ, რომელიც ამავე კომპიუტერთან იმუშავებს ან დროებით სარგებლობს, უპრობლემოდ დაათვალიეროს თქვენი ელფოსტა და სხვა გვერდები.

არალიცენზირებული ოპერაციული სისტემები - ოპერაციული სისტემების არალიცენზირებულ, პირატულ ასლებში შესაძლოა მავნე პროგრამა აღმოჩნდეს. თუ არ გსურთ ლიცენზირებული პროგრამების ყიდვა, გამოიყენეთ უფასო ანალოგები. გადმოწერამდე გაეცანით, თუ როგორ აფასებენ მათ უსაფრთხოებას საიმედო ინტერნეტ რესურსებზე.
ავტომატური განახლების რეჟიმი - ელექტრონულ მოწყობილობაში პროგრამები განახლების რეჟიმში უნდა მუშაობდეს. მათ უახლეს ვერსიებში, დიდი ალბათობით, რიგი ფუნქციები გაუმჯობესებული იქნება, გაუმჯობესებული იქნება ასევე უსაფრთხოების გარანტიებიც.

ვირუსიანი ინფორმაციის გადამტანები - მოერიდეთ თქვენს კომპიუტერზე ინფორმაციის უცნობი გადამტანების შეერთებას (როგორიცაა მეხსიერების ბარათი, SD-ბარათები, სმარტფონი), თუნდაც დატენვის მიზნით. ამგვარი მოწყობილობები შესაძლოა მავნე პროგრამას ატარებდნენ.
გამორთეთ უცხო მოწყობილობებისთვის ავტომატური გადმოწერის ფუნქცია. ეს თავიდან აგაცილებთ ამ მოწყობილობებში არსებული პროგრამების თქვენს კომპიუტერში გადმოტანის შესაძლებლობას.

უსაფრთხო დატენვა - არ დატენოთ თქვენი ტელეფონი და პლანშეტი ყველა ხელმისაწვდომ ადგილას. ამით შესაძლოა თქვენი მოწყობილობა დაუკავშიროთ დავირუსებულ პროგრამას, რომელმაც, შესაძლოა, თქვენი მონაცემები ჩაიგდოს ხელში. საერთო გამოყენების დამტენები (რომლებიც კიოსკებივით ან ყუთებივით გამოიყურება) მხოლოდ უკიდურეს შემთხვევაში გამოიყენეთ, რადგან დენის წყაროს გარდა, ისინი შესაძლოა სხვა ქსელსაც უკავშირდებოდეს. ამიტომ, სასურველია, მოძებნოთ ჩვეულებრივი ჩამრთველი და თქვენივე დამტენი შეაერთოთ მასში.

საკუთარი კომპიუტერის გამოყენება საერთო სივრცეში - თუ ნოუთბუქით ან კომპიუტერით საზოგადოებრივი თავშეყრის ადგილზე მუშაობთ და მცირე ხნით გსურთ სამუშაო ადგილის დატოვება, მოწყობილობა აუცილებლად გადაიყვანეთ ძილის რეჟიმზე ან დაბლოკეთ ეკრანი. დაბრუნებისას მოწყობილობის ჩასართავად პაროლის შეყვანა მოგიწევთ. თუ საზოგადოებრივი თავშეყრის ადგილას დაყენებულია სათვალთვალო კამერები, არ ღირს რაიმე ტიპის პაროლის შეყვანა. ზოგადად, ამ დროს, ინტერნეტ სერვისები ძალიან ფრთხილად უნდა გამოიყენოთ.

უფასო, დაუცველი Wi-Fi - ხალხმრავალ ადგილზე დაუცველ Wi-Fi-ისთან გამოიყენეთ VPN. ხშირ შემთხვევაში, ჰაკერები სწორედ საზოგადოებრივ Wi-Fi-ისთან დაკავშირებული კომპიუტერებიდან ახერხებენ ინფორმაციის მოპოვებას.

ადმინისტრატორის ანგარიშის გამოყენება - Windows-იან კომპიუტერებზე არ ღირს ადმინისტრატორის უფლების მქონე ანგარიშით მუშაობა. უმჯობესია, რიგითი

მომხმარებლის ანგარიშით ისარგებლოთ და, თუ უცხო პროგრამა ეცდება თქვენი თანხმობის გარეშე რაიმე პროგრამის დაყენებას, მაშინ Windows შეგატყობინებთ, რომ უსაფრთხოებისთვის აუცილებელია ადმინისტრატორის ანგარიშიდან პაროლის შეყვანა.

კომპიუტერის თხოვება - ელფოსტის შემოწმების ან Skype-ით სარგებლობის მიზნით, ნუ გადასცემთ უცხო პირებს თქვენს კომპიუტერს. თუ მაინც მოგიწევთ ამის გაკეთება, წინასწარ გააქტიურეთ სტუმრის გვერდით, საიდანაც თქვენს კომპიუტერში ახალი პროგრამის დაყენება არ იქნება შესაძლებელი.

ონლაინ თაღლითობა - უფრთხილდით წერილებს, სადაც გთხოვენ პირად, ასევე, სარეგისტრაციო მონაცემებს. გარდა ამისა, არავითარ შემთხვევაში არ გახსნათ უცნობი წყაროსგან მიღებულ საეჭვო წერილებში არსებული ბმულები. წინააღმდეგ შემთხვევაში, შესაძლოა, ონლაინ თაღლითობის (internet phishing) მსხვერპლი გახდეთ.

ანტივირუსი - აუცილებლად ისარგებლეთ ანტივირუსით. ბევრ გავრცელებულ ანტივირუსულ პროგრამას აქვს უფასო ლიცენზია, რომელიც სავსებით საკმარისია რიგითი მომხმარებლისთვის. მაგალითად, AVG ან Avast. არ დაგავიწყდეთ მისი მუდმივად განახლება.