

დიმიტრი ხეთაგური

პუბლიკაცია



ზნელ ქსელში პერსონალური ინფორმაციის გამოყენების  
პრობლემები

ინფორმაციული ტექნოლოგიები

თბილისი

2022

## ანოტაცია

ამ ეტაპზე კაცობრიობის მზარდმა მოთხოვნილებამ ბაზარზე განაპირობა ახალი ტექნოლოგიების შექმნისა და არსებული ტექნოლოგიების გაუმჯობესების აუცილებლობა. მსოფლიოს წამყვანი ქვეყნები ცდილობენ მაქსიმალურად განავითარონ და ხელი შეუწყონ ამ სფეროს, რადგან ტექნოლოგიური სფერო არის მსხვილი სექტორი, რომელსაც აქვს დიდი შემოსავალი და დასაქმების მაღალი პოტენციალი. ის აკავშირებს სხვადასხვა ბიზნეს სექტორებს, რაც ქვეყნებს საშუალებას აძლევს განვითარდნენ მრავალი მიმართულებით.

სწორედ ერთი-ერთი მიმართულებაა კიბერუსაფრთხოება, ხოლო კიბერ უსაფრთხოებაში დარქვების განხრა, რომელიც იბრძვის ბნელ ქსელში პერსონალური ინფორმაციის გაჟონვის წინააღმდეგ.

## Annotation

At this stage, the growing demand of mankind in the market has necessitated the creation of new technologies and the improvement of existing technologies. Leading countries of the world try to develop and promote this field as much as possible, because the technology field is a large sector with high incomes and high employment potential. It connects different business sectors, allowing countries to develop in many directions. One of the directions is cyber security, while cyber security is a diversion that fights against the leakage of personal information in a dark network.

## სარჩევი

ანოტაცია.....	2
შესავალი.....	4
თავი 1. ვებ ტექნოლოგიების და კიბერუსაფრთხოების სისტემები	
1.1 Web Browsers - ვებ-ბრაუზერები .....	5
1.2. ბნელი ქსელი - DarkWeb, DarkNet, DeepWeb.....	9
1.3. ბნელი ქსელის საზოგადოება - Community.....	10
1.4. კიბერ უსაფრთხოება და ინფორმაციული ტექნოლოგიები.....	13
თავი 2. სტრატეგიული კიბერშეტევებისგან თავდაცვის საშუალებები	
2.1 კიბერ შეტევის მექანიზმები.....	16
2.2 პერსონალური ინფორმაცია.....	22
2.3 პრობლემის აღმოფხვრა.....	26
2.4 პროექტი.....	28
დაკსვნა.....	34
გამოყენებული ლიტერატურა.....	35

## შესავალი

XXI საუკუნე წარმოადგენს ინფორმაციული ტექნოლოგიების გამოწვევების ეპოქას, სადაც უმნიშვნელოვანესი და საყურადღებოა პერსონალური ინფორმაციული უსაფრთხოება.

ახალი ტექნოლოგიური გამოგონებები, მიღწევები, ყველაფერი რაც ქსელშია ჩართული ეფუძნება პერსონალურ ინფორმაციას ანუ შეგვიძლია ვთქვათ, რომ ყველაფრის ტექნოლოგიური საფუძველი მონაცემები.

აღსანიშნავია, რომ ინფორმაციული ტექნოლოგიების სფეროს მიეკუთვნება, საკომუნიკაციო საშუალებები, ტექ საშუალებები, რობოტები, კრიპტოები, მანქანა-დანადგარები და ასე შემდეგ.

ზემო აღნიშნული ინფორმაციიდან გამომდინარე საბაკალავრო ნაშრომში ძირითადი ყურადღება მექნება პერსონალურ ინფორმაციის გამოყენების პრობლემაზე ბნელ ქსელში, თუ როგორ შეიძლება ვიყოთ ინტერნეტ სივრცეში და მითუმეტეს ბნელ ქსელში ანონიმურები, ვიმოდრაოთ საიტებზე უსაფრთხოდ და არ შეექმნას პრობლემა ჩვენ პერსონალურ ინფორმაციას, რომელიც დღევანდელ ცხოვრებაში ყველაზე ძვირადღირებულია.

ამ და სხვა პრობლემებმა გამოიწვია მსოფლიოს მასშტაბით ჩამოყალიბებულიყო თავდაცვის სფეროს ახალი თანამედროვე მექანიზმი რომელსაც ეწოდა კიბერ და ინფორმაციული უსაფრთხოება. სხვადასხვა სექტორების, ბიზნესების თუ სპეც. სამსახურების მთავარ ამოცანას პირველ რიგში წარმოადგენს სწორედაც რომ პერსონალური ინფორმაციის შენახვა, უსაფრთხოება და არქივაცია.

# თავი 1. ვებ ტექნოლოგიების და კიბერუსაფრთხოების სისტემები

## 1.1. Web Browsers - ვებ-ბრაუზერები

XX საუკუნიდან მეცნიერებმა დაიწყეს ექსპერიმენტები ელექტრონიკის დარგში. გამოიგონეს ელექტრონული ლამპები, რომელთაც შეედლოთ ემართათ ელექტროდების სუსტი ნაკადი, შემდეგ შეიქმნა პლატები, სქემები, კავშირგაბმულობა. ნელ-ნელა დაიხვეწა ტექნოლოგიაც და XX საუკუნიდან დიდი გარდატეხები მოხდა ინფორმატიკის დარგში სადაც შემუშავდა უკვე გამართული კომპიუტერების წარმოება, ინფორმაციის დამუშავების მეთოდები და ფიზიკურ-მათემატიკური ფორმულირება, კომპიუტერის გამართული აგებულების, რომელიც ოთახის ხელა აღარ იქნებოდა და ჩამოყალიბდა ხელით სატარებელი მოწყობილობის ზომამდე.

კომპიუტერის განვითარების შემდეგ მასში შემავალი ელემენტების განვითარებაზე, მეცნიერებთან ერთად მუშაობა დაიწყო როგორც დიდმა კომპანიებმა ასევე საზოგადოებამ. XX საუკუნის მიწურულს კი გამოჩნდა კომპიუტერში ინტერფეისები, ხოლო ინტერფეისებში ინტერნეტ სივრცეში სამოძრაო გარემო სახელწოდებით **Browser - ბრაუზერი**.

ინტერნეტში გამოჩნდა ბრაუზერი სახელწოდებით Explorer, რომელსაც აწარმოებდა კომპიუტერის მწარმოებელი კომპანია და ქარხნულადვე მოჰყვებოდა მას. შემდეგ განვითარებასთან ერთად ჩამოყალიბდა სხვადასხვა კატეგორიის ბრაუზერები, რომლებიც განსხვავებულ მონაცემებს მოითხოვდნენ გამართული მუშაობისთვის (საუბარია კომპიუტერულ აგებულებაზე).

ბაზარზე გამოჩნდნენ კომპანიები, რომლებიც აწარმოებდნენ სხვადასხვა ბრაუზერებს: Opera, Google Chrome, Mozilla Firefox და ასე შემდეგ. სწორედ ბრაუზერში გაშვებული არქიტექტურული პროექტი კი გახდა ერთ-ერთი საკომუნიკაციო საშუალება, მაგრამ აქვე გამოიკვეთა იმის პრობლემა, რომ საჭირო იყო უსაფრთხოების ჩარჩოების შემოღება და კომუნიკაციის დაშიფვრის პუნქტების მოფიქრება. შემდეგ აქვე შემოიღეს სწორედ იმ დაშიფვრების მეთოდები, როგორიცაა AES, Base64, Bip, Hex და ვებ გადაცემათა პროტოკოლები SSL, TLS და ასე შემდეგ.

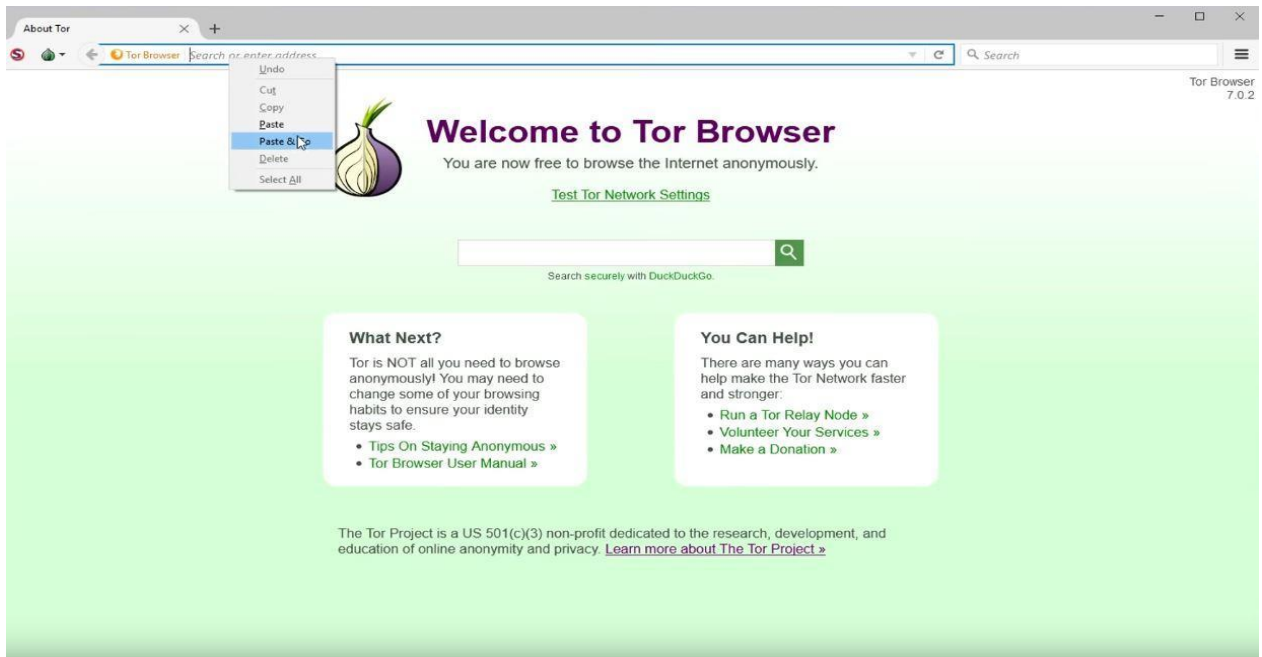
ამ ყველაფერს საზოგადოება კი ჩვეულებრივ მოიხმარდა, მაგრამ სახელმწიფო უსაფრთხოების, უშიშროების და სპეცსამსახურებიც ასე მარტივად ამ პროტოკოლებს ვერ მოერგებოდნენ და სწორედ აქ ჩნდება სახელმწიფო საიდუმლო პროექტი TOR.

აშშ-ის საკომუნიკაციო საშუალებად ბრაუზერი ტორი იგივე Project TOR Browser ჩამოყალიბდა, რომლითაც სარგებლობდნენ ამერიკის სამართალდამცავი უწყებების თანამშრომლები.

TOR - ბრაუზერის მუშაობის პრინციპი შემდეგშია, მოწყობილობა უერთდება ბრაუზერს და ხდება მთლიანი მოწყობილობის იდენტიფიკაცია ტორის მხრიდან თუ რა მოწყობილობაა, რა აიპი მისამართი აქვს, რომელ სისტემას იყენებს, რომელი ქვეყნიდანაა, რომელ სასაათო სარტყელშია, ეს აიპი კიდევ რომელ ბრაუზერს იყენებს, რომელი ოპერაციული სისტემაა და ასე შემდეგ. მოკლედ რომ ვთქვათ ტორ ბრაუზერი დეტალურად იღებს ინფორმაციას თუ მონიტორს რა გაფართოება აქვს.

მსგავსი პროექტის საზოგადოებაში ჭორის გავრცელების შემდეგ უკვე 2002 წელს, პროექტი გამოქვეყნდა საჯარო და ყველასთვის ხელმისაწვდომი გახდა, სწორედ აქედან იწყება უკვე ბნელი ქსელის წარმოშობა, მსოფლიოს უდიდესი პროექტის საკაცობრიო რეალიზება და მასშტაბური მუშაობა ყველასთვის საყვარელი ანონიმური ბრაუზერისთვის, სადაც ერთიანდებიან სხვადასხვა კუთხეში მყოფი დევლოპერები და იწყებენ ისეთი ბრაუზერის, სისტემის შემქნას რომელიც კიბერ თავისუფლებას ხელს შეუწყობს და ჩაახშობს პერსონალურ იდენტიფიკაციას.

სწორედ TOR ბრაუზერი გახდა დამოუკიდებელი პროექტი, რომლის განვითარებაშიც მონაწილეობს უამრავი უცნობი დევლოპერი და წარმოადგენს დიდ ნაბიჯს ანონიმური სივრცის განვითარებისთვის.



ბრაუზერ ტორს მალევე ჩამოუყალიბდა დომეინები, ძრავები, ინტერფეისები, რომლებიც ზრუნავენ ვიზიტორების იდენტიფიკაციაზე სხვადასხვა ქსელში, მაგალითად თუ თქვენ შეხვალთ ტორის ვებ-გვერდზე თქვენ ნახავთ, გაფრთხილებას რომ გთხოვთ ჩართოთ VPN (Virtual Private Network), რომელიც დამალავს თქვენს რეალურ აიპი მისამართს და თქვენი იდენტიფიცირება გართულდება. მაგრამ თუ თქვენ VPN კავშირს არ გამოიყენებთ და პირდაპირ დაუკავშირდებით ბრაუზერს, მაშინ თქვენ აიპი შეუერთდება ტორში გაშვებულ პროქსს, სადაც თავმოყრილია თქვენნაირი ასობით აიპი მაგრამ თქვენი იდენტიფიცირება გაცილებით მარტივი ხდება ვიდრე VPN კავშირით.

- რა არის IP?

IP-მისამართი უნიკალური ნომერია, მსგავსად საიდენტიფიკაციო მისამართისა, რომელიც დაკავშირებულია ინტერნეტში თქვენს მოქმედებებთან, ასევე IP - მისამართი იყოფა კიდევ რამდენიმე კატეგორიად, როგორიცაა გარე მისამართი, შიდა მისამართი, მაკ ადრესი, ინტერნეტის მიწოდების მისამართი, ფაილის გაზიარების მისამართი და ასე შემდეგ.



საინტერესოა, რომ ინტერნეტ სერვის მომწოდებლებთან ყოველი აიპი და მაკ მისამართის მოქმედება 24/7 ფიქსირდება და არ არის შექმნილი სისტემა, რომელიც გამოავლენს პოტენციურ დამნაშავეს და შემდეგ სახელმწიფო ორგანო მიიღებს შესაბამის ზომებს, პოტენციური დაზიანებისგან ან კიბერ შეტევისგან დასაცავად.



## 1.2. ბნელი ქსელი - DarkWeb, DarkNet, DeepWeb

ბნელი ქსელის კატეგორიები, რა განსხვავება მათ შორის და რა დანიშნულება აქვს სხვადასხვა კატეგორიის ბნელ ქსელში მოძრაობას, რა შედეგები შეიძლება მოიტანოს ჩვენთვის და რამდენად უსაფრთხოა....

როგორც ზემოთ აღნიშნული მაგალითებზე ვიგებთ, ბნელი ქსელი შეიქმნა გარკვეული საზოგადოებისთვის და არ იყო მისაწვდომი ყველასთვის გარკვეული პერიოდის განმავლობაში, მაგრამ უკვე ყველასთვის მისაწვდომია და რითაც ცნობილია ბნელი ქსელი, იქ მიმდინარე კიბერ კრიმინალის უდიდესი ინფორმაციული მიმოცვლაა.

DarkWeb - დარქ ვები წარმოადგენს მარტივად მისაღწევად ანონიმურ საიტებს, რომელიც რეგისტრირებულია ჩვენთვის ხილულ ღია სივრცეში. ანუ ჩვეულებრივი ნებისმიერი ბრაუზერითაც კი შეგვიძლია დარქვების დათვალიერება და ინფორმაციის მიღება, ხოლო რაც შეეხება DarkNet და DeepWeb ქსელის ტიპებს აქ უკვე მთავარ როლში შემოდის შუამავალი ბრაუზერი ტორი TOR - სადაც მის გარეშე იქ ვერ მოვხვდებით ესენი წარმოადგენენ ტორ საიტების ონიონის დომეინ დაბოლოებებს მაგალითად (web.onion), სადაც სხვა ბრაუზერით ჩვენ წვდომის უფლება არ გვაქვს.

ამ ყველა ქსელში შექმნილია სხვადასხვა საიტები და მიმდინარეობს სხვადასხვა ინფორმაციების მიმოცვლა, მაგალითად არის ფორუმი ჰაკერებისთვის, ფორუმი ნარკოტიკებისთვის, იარაღებისთვის, ქილერებისთვის, საიდუმლო გაჟონილი ინფორმაციებისთვის და ასე შემდეგ. აქ თავმოყრილია ყველა ის ვებ-გვერდი, რომელსაც ჩვენთვის ხილულ ზედაპირულ ქსელში ბლოკავენ სამთავრობო და სპეც. უწყებები.

### 1.3. ბნელი ქსელის საზოგადოება - Community

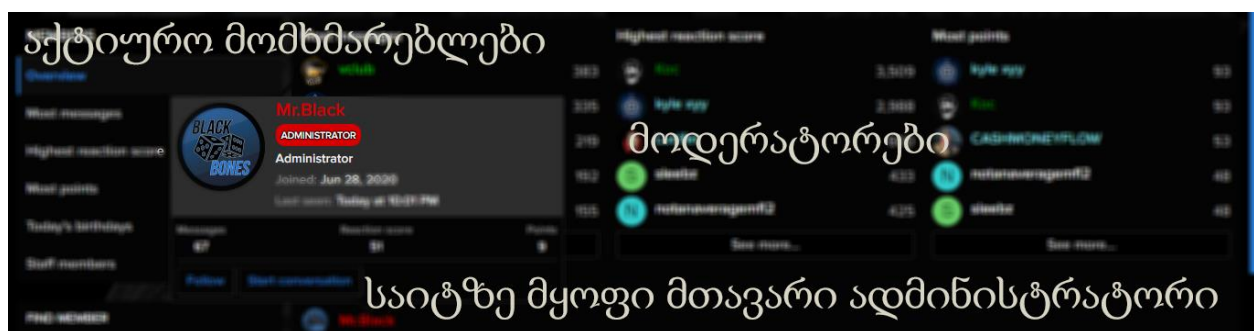
ბნელი ქსელის ფორუმებზე თავმოყრილია სხვადასხვა კატეგორიის ხალხი, რომელთა ძირითადი მიზანია რთულად მიღწევადი ინფორმაციების მოძიება, მაგალითად ფორუმები, ბლოგები, სიახლეები და ასე შემდეგ.

ბნელი ქსელის ფორუმებზე ძირითადად დიდი მოთხოვნა სწორედ, რომ პერსონალურ ინფორმაციებზეა და რა თქმა უნდა ყიდვა-გაყიდვა კრიპტოვალუტებში მიმდინარეობს.

უფრო, რომ განვავრცოთ და გავხსნათ სისტემა ასე მუშაობს ბნელი ქსელის ერთი ჩვეულებრივი ფორუმის სისტემა:

ფორუმზე რეგისტრირებულია ადმინისტრატორი, მოდერატორი, ედიტორი და გააჩნია კიდევ როგორ აქვს ადმინისტრაციას დაწერილი საიტის შინაგანაწესი.

ადმინისტრატორი აკონტროლებს ვებ-გვერდს და ინფორმაციებს, მოდერატორი აკონტროლებს იქ განვითარებულ კონტენტს, ვალიდურობას და უსაფრთხოებას რომელიც შეეხება ფორუმს. ასევე, მომხმარებელთა აქტივობას და ახალი მომხმარებლების წახალისების აქტივებს. ედიტორი კი აკონტროლებს განთავსებული კონტენტის შიგთავსს ზრუნავს მისი სწორი ადგილის განაწილებაზე და აკონტროლებს ცენზურას ან კონკრეტულ წესის დარღვევის წინაპირობის საშიშროებას.



აღსანიშნავი ფაქტია, რომ პერსონალურ ინფორმაციაზე ერთ-ერთი ყველაზე დიდი მოთხოვნა ბნელ ქსელში ეგრეთწოდებულ ლიდებზეა, ანუ აფილაციაზე.

ეს არის შეგროვებული პერსონალური ინფორმაცია, მონაცემთა ბაზა, სადაც გაერთიანებულია გარკვეულ სფეროში მოღვაწე ან გარკვეულ ქვეყანაში მცხოვრები ხალხის სახელი, გვარი, პირადი ნომერი, საკონტაქტო ნომერი, საცხოვრებელი ინფორმაცია და ა. შ. პერსონალური ინფორმაციით ვაჭრობა წარმოადგენს ერთ-ერთ დიდ ბიზნესს ბნელ ქსელში. ძირითადი მოპოვება ხდება ისეთ სექტორებში, როგორიცაა კრიპტოვალუტის ბირჟების გატეხვა, ყალბი კრიპტო ან საბანკო ვებ-გვერდების შექმნა და გავრცელება, ცნობილი ფინანსური კომპანიების საიტების კლონირება და გავრცელება. ასევე ქოლ-ცენტრებში, სადაც ტრიალებს ეგრეთწოდებული ცხელი და ცივი ლიდები.

*ლიდი - ეწოდება პიროვნებას ვისაც ურეკავენ გარკვეული სექტორის სახელით და აბანდებინებენ ფულს ისეთ საქმეში, სადაც ჰპირდებიან მომგებიან აქციებს, მაგრამ სამომავლოდ მასთან კავშირს წყვეტენ.*

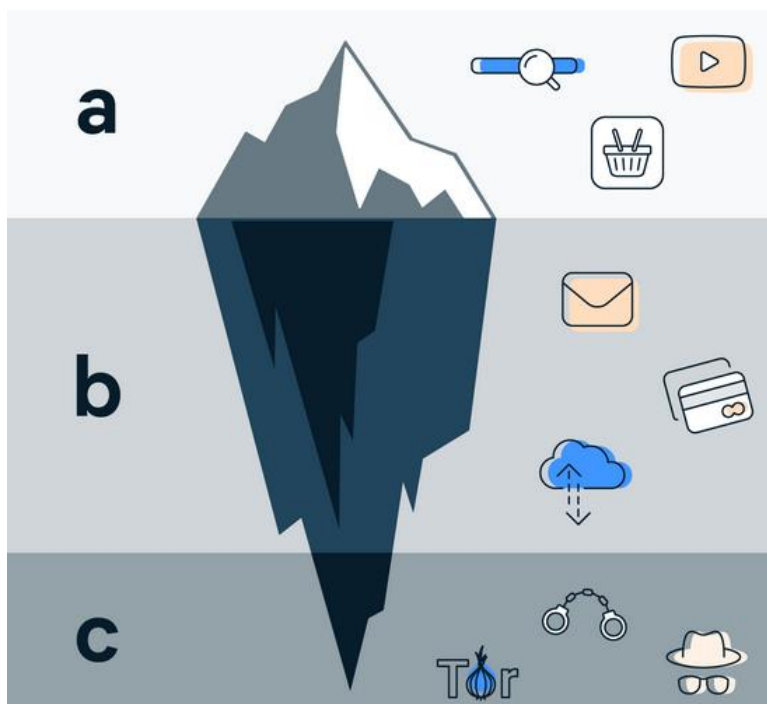


აღსანიშნავი ფაქტია, რომ ბნელ ქსელში არსებობს გარკვეული წოდებები გარდა ადმინისტრაციისა, რომლებსაც კიდევ სხვა გარკვეული პრივილეგიები და უფლებები აქვთ. მაგალითად არის წოდება VIP, რომელიც შეიძლება მომხმარებელმა მიიღოს როგორც აქტიურობის ნიადაგზე ასევე თანხის სანაცვლოდ, სამაგიეროდ კი ნახავს დახურულ და

საიტზე განთავსებულ შეზღუდულ და ყველასთვის მიუწვდომელ კონტენტს, რომლის გამოყენება იმაზეა დამოკიდებული, თუ როგორ გამოიყენებს იგი ამ ინფორმაციას.

ბნელ ქსელში ყველაზე დიდი აქტივობა 2021 წლის სტატისტიკის მიხედვით შეინიშნება გატეხილ კრიპტო ანგარიშებზე, საბანკო ანგარიშებზე, გამომძალველ კრიპტერ ვირუსებზე, ლიდებზე, სოციალურ ქსელებზე და ნარკოტიკებზე.

2010-დან 2020 წლამდე ყველაზე დიდი მოთხოვნა ფიქსირდებოდა ნარკოტიკებზე, მონებზე, ქალებზე, იარაღზე, შავ ფულსა და შავ კრიპტოვალუტაზე, DDoS პაკეტებზე, ბოტებსა და გატეხილ საიტებზე.



#### 1.4. კიბერ უსაფრთხოება და ინფორმაციული ტექნოლოგიები

ამ ყველაფრიდან გამომდინარე ასპარეზზე გამოდის კიბერ უსაფრთხოება, რომლის მიზანიც, ვალდებულებაც და მამოძრავებელი ძალაც ზემოთაღნიშნული ინფორმაციების გავრცელებისგან დაცვაა. არ გაჟონოს ინტერნეტ სივრცეში მსგავსმა ინფორმაციებმა, არ დაზიანდეს საზოგადოება და ძლიერად იყოს ჩამოყალიბებული ინფორმაციული ტექნოლოგიების პოლიტიკა მოქმედ სექტორებში.

კიბერ შეტევები მსოფლიოს მასშტაბით გამუდმებით მიმდინარეობს, სადაც ტექნოლოგიები შესაძლებლობისამებრ რეაგირებენ დახვეწილ კიბერ შეტევის მექანიზმებზე.



ფოტოზე ასახულია ერთ-ერთი კიბერ რუკა, სადაც ფიქსირებულია კიბერ შეტევების ხაზები, მიმართულებები და რაოდენობა, ასევე სიმძლავრე შედეგი და კიბერ შეტევის შედეგად დაზიანებული წერტილები

კიბერ უსაფრთხოების განვითარება მსოფლიოს მასშტაბით ერთ-ერთი პრივილეგირებული მიმართულებაა, ამაზე მუშაობენ მსოფლიოს უდიდესი ინსტიტუტები, კომპანიები, სახელმწიფოები, სექტორები და ასე შემდეგ.

ტექნოლოგიური განვითარების და მისი უსაფრთხოების გაძლიერებით, მყარ ნაბიჯებს დგამს კაცობრიობა, იხვეწება ტექნოლოგიები, მარტივდება ცხოვრების წესი და ინერგება ავტომატიზაცია, ამ ყველაფერს სჭირდება ძალიან დიდი მუშაობა, დაკვირვება, გამოთვლები, ანალიტიკა და ყველაფერი ის რაც დააფიქსირებს ადეკვატურ ნაბიჯს უკვე გაციფრულებული საზოგადოებისთვის.

ინფორმაციული უსაფრთხოების ისტორიაში 2020 წლიდან მოხდა ყველაზე დიდი გარდატეხა, რაც გამოიწვია კრიპტოვალუტების დიდმა ევოლუციამ და საბანკო სფეროში, ახალი კრიპტო გადახდების მერჩანტების დანერგვამ. ასევე კრიპტო ვალუტების პოლიტიკის შემუშავება, განვითარებამ.

როგორც, ყველა დანარჩენ დარგში აქაც, საზოგადოებისთვის თავიდან უცხო იყო კრიპტო გადახდის სისტემები, მაგრამ მალევე მიხვდა ყველა მისი დაცულობის და ანონიმურობის სიძლიერეს, რის შემდეგაც გახდა მოთხოვნადი მსოფლიოს უამრავ ქვეყანაში, სადაც როგორც ყველა დარგში აქაც გაჩნდა მათი მომხრეები და მოწინააღმდეგეები.

მსოფლიოს მასშტაბით არის აიტი საზოგადოება, რომელიც ეთანხმება კრიპტო სფეროს განვითარებას და ამ საგადასახადო სისტემის რეგულაციის შემუშავებას. არის მეორე კატეგორია, რომელიც არ ეთანხმება კრიპტო ვალუტების რეგულაციებს, დეცენტრალიზაციებს და გლობალურ პოლიტიკას. აქაც არის გარკვეული არგუმენტები, მიზეზები და წინაპირობები, ისევე როგორც სხვა დანარჩენში.

კიბერ უსაფრთხოება ძალიან ძლიერად მიდრეკილია კრიტიკული ინფრასტრუქტურის დაცვაზე, მაგალითად მასაჩუსეტსის ტექნოლოგიური ინსტიტუტის ინტერნეტ პოლისების კვლევების ინიციატივისა (MIT Internet Policy Research Initiative) და საერთაშორისო კვლევების ცენტრის (MIT Center for International Studies) ერთობლივი მუშაობით 2015-2016 წლებში ჩატარდა კრიტიკული ინფრასტრუქტურის სუბიექტების კიბერუსაფრთხოების



გამოწვევების ვორქშოპი. მასში მონაწილეობას იღებდნენ ამერიკის, კანადის, იაპონიისა და ევროპის საკვანძო ინდუსტრიული ფირმების წარმომადგენლები; ასევე სამთავრობო სექტორის, მასაჩუსეტსის ტექნოლოგიური ინსტიტუტისა და კარნეგი-მელონის უნივერსიტეტის წარმომადგენლები.

კრიტიკულ ინფრასტრუქტურად მიიჩნევა ქვეყნისთვის უმნიშვნელოვანესი ისეთი სისტემები და აქტივები (როგორც ფიზიკური ისე ვირტუალური), რომელთა მწყობრიდან გამოყვანა ან განადგურება არსებითად შეასუსტებს ქვეყნის უსაფრთხოებას, ეკონომიკას ან ჯანდაცვას. აშშ-ს საპრეზიდენტო დირექტივა ნომერი 21-ის მიხედვით (PPD-21) ასეთი სულ თექვსმეტია

[Press Briefings](#)

**[Statements & Releases](#)**

[White House Schedule](#)

[Presidential Actions](#)

[Executive Orders](#)

[Presidential Memoranda](#)

[Proclamations](#)

[Legislation](#)

[Pending Legislation](#)

[Signed Legislation](#)

[Vetoed Legislation](#)

[Nominations & Appointments](#)

[Disclosures](#)

## Presidential Policy Directive – Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

### Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

## თავი 2. სტრატეგიული კიბერშეტევებისგან თავდაცვის საშუალებები

### თავი 2.1. კიბერ შეტევის მექანიზმები

ინფორმაციული ტექნოლოგიების განვითარების სტიმულატორი სწორედ რომ საზოგადოების მოთხოვნაა უფრო ძლიერ ტექნოლოგიებზე. ანუ პროდუქტის მეტი მოთხოვნა იწვევს მისი რეალიზების გამარტივებულ და გაძლიერებულ ფორმულირებას, კიბერ შეტევების გახშირება იწვევს მისგან თავის დახვეწის მეთოდების გაძლიერებას, შეტევების უამრავი მეთოდია, რომლებიდანაც ყველა ხშირად გვხვდება, კიბერ შეტევის მეთოდი: Phishing, DDoS, Crypters. ეს ის სამი შეტევის ტიპია, რომელიც ინტერნეტში ყველაზე ხშირად ჩნდება სხვადასხვა მოწყობილობებში. ასევე არსებობს შეტევის კიდევ სხვა ტიპებიც, როგორიცაა:

**Passive Attack პასიური შეტევა** - პასიური შეტევის დროს ხდება ქსელის დაუცველი ტრაფიკის მონიტორინგი იმისათვის, რომ იპოვონ და ამოიღონ პაროლები და ინფორმაცია, რომელიც შეიძლება გამოყენებული იყოს სხვა ტიპის შეტევების განსახორციელებლად. პასიური შეტევები მოიცავენ ტრაფიკის ანალიზს, დაუცველი კომუნიკაციების მონიტორინგს, სუსტად დაშიფრული ტრაფიკის დეშიფრაციასა და ისეთი აუთენტიფიკაციის ინფორმაციის მიღებას, როგორიცაა მაგალითად პაროლები ან ელექტრონული მისამართები. ქსელის ოპერაციების პასიური შეტევა მოწინააღმდეგეებს საშუალებას აძლევს დაინახონ მომავალი ქმედებები. პასიური შეტევა იწვევს ინფორმაციის ან მონაცემთა ფაილების გამჟღავნებას მომხმარებლის თანხმობის ან ცოდნის გარეშე.

**Active Attack - აქტიური შეტევა** - აქტიური შეტევის დროს ჰაკერი ცდილობს დაცულ სისტემებზე შეტევას. ეს შეიძლება გაკეთდეს სტელსით, ვირუსებით, ჭიებით ან ტროას ცხენების გამოყენებით. ეს შეტევები მიმართულნი არიან ქსელის ხერხემალზე (backbone) და ცდილობენ სატრანზიტო ინფორმაციის გამოყენებას ან მოახდინონ დისტანციური თავდასხმა ავტორიზებულ მომხმარებელზე. აქტიური შეტევა იწვევს



მონაცემთა ფაილების გამჟღავნებას ან გავრცელებას, DoS-ის მატებას ან მონაცემების მოდიფიკაციის ცვლილებას.

**Distributed Attack** განაწილებული შეტევა - განაწილებული შეტევის დროს ჰაკერმა უნდა შესთავაზოს სისტემას რაიმე კოდი, მაგალითად Trojan horse-ს ან back-door პროგრამა, ისეთნაირად, რომ სისტემამ ჩაითვალოს ეს კოდი დაცულად და შემდგომ განაწილოს ის სხვა კომპანიებსა და მომხმარებლებს შორის. ასევე განაწილებული შეტევები ფოკუსირებენ ტექნიკის ან პროგრამული უზრუნველყოფის ზიანის მომტანი მოდიფიკაციას ქარხანაში ან დისტრიბუციის დროს. ზიანის მომტანი კოდი შემდგომში გამოიყენება იმისათვის, რომ მიიღოს არავტორიზებული წვდომა ინფორმაციასთან ან სისტემური ფუნქციებთან

**Insider შეტევა** - insider-თა შეტევის დროს კომპანიის თანამშრომელი ახორციელებს შეტევას სისტემაზე. insider შეიძლება იყოს ზიანის მომტანი ან არა. ზიანის მომტანი insider შეგნებულად ისმენს, იპარავს ან აზიანებს ინფორმაციას, იყენებს მას არაკანონიერად ან ბლოკავს სხვა ავტორიზებულ მომხმარებლებს. არაზიანისმომტანი შეტევები ხშირად ხდება დაუდევრობის, არცოდნისა ან უსაფრთხოების გაუთვალისწინებლობის გამო დავალების შესრულების დროს.

**Close-in Attack** - Close-in შეტევის დროს ჰაკერი ცდილობს ფიზიკურად მიუახლოვდეს ქსელის კომპონენტებს, მონაცემებსა და სისტემებს რათა მეტი გაიგოს ქსელის შესახებ. ამ შეტევის დროს იგი უნდა მიუახლოვდეს სისტემებსა და data-ცენტრებს იმისათვის, რომ შეცვალოს, შეკრიბოს ან დაბლოკოს ინფორმაციაზე წვდომა.

**Social Engineer - სოციალური ინჟინერია** - ერთ-ერთი პოპულარული შეტევის გზა არის სოციალური ინჟინერია, რომლის დროს ჰაკერი ინფორმაციულ სისტემებთან წვდომას იღებს მოტყუებით პირადი ურთიერთობის დროს, ელექტრონული წერილებით ან სატელეფონო საუბრებში. სოციალური ინჟინერიის მთავარი იდეა მდგომარეობს იმაში, რომ ჩავსვით ადამიანი ქსელის დარღვევის ციკლში და გამოვიყენოთ ის იარაღად. ინფორმაცია რომელსაც მსხვერპლი გასცემს შეიძლება გამოყენებული იქნას შემდგომი შეტევისთვის და სისტემაში შეღწევის ავტორიზაციის მიღებისთვის. მომხმარებელი ყოველთვის

მოხსენიებული არის, როგორც ყველაზე სუსტი ბმული ქსელის უსაფრთხოებაში.

**Phishing შეტევა** - Phishing შეტევის დროს ჰაკერი ქმნის ყალბ ვებ გვერდს, რომელიც გამოიყურება ზუსტად როგორც რეალური პოპულარული საიტი, როგორც მაგალითად facebook-ის პირველი გვერდი. ამის შემდეგ ჰაკერი უგზავნის მომხმარებელს წერილს, რომელშიც არის ბმული ამ ყალბ გვერდზე. როდესაც user გადადის ამ საიტზე და შეიყვანს პირად ინფორმაციას, ჰაკერი მიიღებს წვდომას ამ ინფორმაციაზე და ეცდება გამოიყენოს რეალურ საიტზე.

**Sniffing სნიფინგი** - ქსელური პაკეტების სნიფინგი არის ქსელში გამავალი მონაცემთა პაკეტების მოსმენა და აღება. სნიფერული პროგრამა მუშაობს ქსელის Ethernet დონეზე და იღებს მთლიან შემავალ და გამავალ ტრაფიკს. თუ Ethernet-ის პლატა ძეხნის რეჟიმშია სნიფერის პროგრამა მიიღებს უფრო მეტ ინფორმაციას ტრაფიკიდან. სნიფერს, რომელიც დაყენებულია ქსელის ხერხემალ მოწყობილობაზე ან ქსელის აგრეგაციის წერტილზე, საშუალება აქვს ქსელის მთლიანი ტრაფიკის მონიტორინგის. სნიფერების უმრავლესობა არის პასიური, ისინი პასიურად უსმენენ მოწყობილობის ქსელურ ინტერფეისში შემავალ და გამავალ მონაცემების პაკეტებს. ინტერნეტში არსებობს უამრავი სნიფერული პროგრამა. მათგან ყველაზე დახვეწილი უფრო აქტიური შეტევის საშუალებას გვაძლევს. სნიფინგიდან ყველაზე საუკეთესო დაცვაა end-to-end ან user-to-user ტრაფიკის შიფრაცია.

**Man in the middle attack გატაცებითი შეტევა** - ეს ტექნიკა იყენებს TCP/IP პროტოკოლის არქიტექტურაში არსებულ სისუსტეებს. გატაცება ხდება როდესაც ვიღაც ერევა და აკონტროლებს თქვენი კომუნიკაციის პროცესს. როდესაც კომპიუტერები ურთიერთობენ ქსელის დაბალ დონეებზე, მათ შეიძლება ვერ დაადგინონ სწორად ვისთან ცვლიან მონაცემებს. თქვენ ფიქრობთ, რომ საუბრობთ ორიგინალურ პარტნიორთან, მაგრამ რეალურად ყველა პირად ინფორმაციას ხედავს ჰაკერი

**Spoof შეტევა spoofing** - შეტევის დროს ჰაკერი ცვლის გამოგზავნილი მონაცემთა პაკეტების წყაროს მისამართს ისე, რომ პაკეტები გამოჩნდეს, როგორც სხვა წყაროდან გამოგზავნილი. ეს შეიძლება firewall წესების შემოვლითი გზებით გავლის მცდელობა იყოს. ქსელში ყველა ჩართული მოწყობილობა აუცილებლად აგზავნის IP მისამართებს ქსელში.

ასეთი ინტერნეტ მონაცემების პაკეტები ინახავენ გამომგზავნის IP მისამართს და აპლიკაციის დონის მონაცემებს. თუ ჰაკერი მიიღებს კონტროლს ქსელში გაშვებულ პროგრამულ უზრუნველყოფაზე, ის ადვილად შეძლებს შეცვალოს მოწყობილობის პროტოკოლები იმისათვის, რომ განათავსო თვითნებური IP, მისამართი მონაცემთა პაკეტის წყაროს მისამართის ველში. ეს ტექნიკა ცნობილია, როგორც IP spoofing, რომელსაც შეუძლია ყველა პაკეტის წყაროს მისამართის შეცვლა სხვა ნებისმიერ მისამართზე. პაკეტში შეცვლილი წყარო IP მისამართით ძნელია დავადგინოთ რეალურად ვინ გამოაგზავნა მონაცემები. Spoofing-თან დაცვა არის მისამართების ფილტრაცია, რაც შესაძლებელია როუტერის სწორი კონფიგურირებით. როუტერები ამოწმებენ IP მისამართიდან მიღებულ დატაგრამებს და განსაზღვრავენ არიან თუ არა მისამართები იმ მისამართებს შორის, რომლებიც არიან ინტეფეისით მისაწვდომი. თუ წყარო მისამართი გამომგზავნის პაკეტში არ არის დაშვებული სივრციდან, მაშინ ასეთ პაკეტებს როუტერი ბლოკავს.

**Denial-of-Service შეტევა (DoS)** - მომსახურებაზე უარის თქმის შეტევა არის სპეციალური ტიპის შეტევა, რომელიც მიზნად ისახავს დიდი საიტების გატეხვას. ამ ტიპის შეტევა ქსელში შექმნილია იმისთვის, რომ გამოიყვანოს ქსელი მწყობრიდან დიდი რაოდენობის უსარგებლო ტრაფიკის გამოგზავნით. მომსახურებაზე უარის თქმა ხდება როდესაც ისეთი სისტემა როგორიცაა ვებ სერვერი გადაივსება არალეგიტიმური მოთხოვნებით და ამით არ მისცემს მას საშუალებას ლეგიტიმურ მოთხოვნების უპასუხოს.

**Distributed-Denial-of-Service (DDoS)** - DDoS შეტევა ხდება როდესაც რამოდენიმე გატეხილი სისტემა ან რამოდენიმე ჰაკერი ერთროულად აკეთებს ბევრ მოთხოვნას სერვერზე და ტრაფიკის ავსებით ბლოკავს სერვისს. DDoS-ის დროს ჰაკერმა ჯერ უნდა მიიღოს წვდომა დიდი რაოდენობის ინტერნეტ ჰოსტებთან. ამის შემდეგ ის აყენებს ამ ჰოსტებზე შემტევ პროგრამას, რომელიც მშვიდად ელოდება ბრძანებას control პროგრამიდან, რომელსაც თავის მხრივ აქვს საშუალება დაუკავშირდეს ყველა ჰოსტზე დაყენებულ პროგრამას, მიუთითოს შეტევის სამიზნე და ერთდროულად ამ სამიზნეზე გაუშვას შეტევა. შედეგად კოორდინირებული შეტევა განსაკუთრებით ზიანის მომტანია, რადგან ერთდროულად მოდის ბევრი ჰოსტიდან. როუტერების აქვთ წვდომის ფილტრი,

რითაც შეუძლიათ DoS შეტევის ფილტრაცია და ისიც მცირე მოცულობით, ამიტომ DDoS არის ერთ-ერთი ყველაზე მარტივი და პოპულარული შეტევის ტიპი.

**Buffer overflow ბუფერის გადავსება** - არის, როდესაც ჰაკერი აგზავნის აპლიკაციაში უფრო მეტ მონაცემს ვიდრე ის ელოდება. ბუფერის გადავსების შეტევა როგორც წესი, იწვევს სიტუაციას როდესაც თავდამსხმელი იძენს ადმინისტრაციულ უფლებებს shell-ზე, სადაც shell(შელი) წარმოადგენს მომხმარებლის პრივილეგიით ატვირთულ პლატფორმას იგივე მავნე კოდით დაწერილ პროგრამას, რომელიც ზრუნავს, მომხმარებელმა ანუ ავტორმა მიიღოს ადმინისტრაციის პრივილეგია და სერვერზე არსებული ყველა ბრძანება გაეშვას როგორც საიტის ადმინისტრაციის პრივილეგიით.

**Smurf შეტევა** - ამ შეტევის დროს თავდამსხმელი აგზავნის IP პინგის მოთხოვნებს მიმღებ საიტზე. ping პაკეტი აღნიშნავს, რომ ის მიმართულია რამდენიმე ჰოსტზე სისტემის შიგნით. პაკეტი ასევე აღნიშნავს, რომ ის არის მოთხოვნა რაიმე სხვა საიტიდან, რომელიც არის მომსახურებაზე უარის თქმის შეტევის სამიზნე. შეტევის შედეგად სამიზნე საიტი მიიღებს დიდი რაოდენობის პასუხებს, რომლებსაც სწორად ვერ დაამუშავებს და თუ მიიღებს საკმარისად ბევრ პასუხს, ჰოსტი შეიძლება გამოვიდეს მწყობრიდან და ვერ მიიღოს რეალური ტრაფიკი.

**SYN floods სინქრონული** - როდესაც კომპიუტერი ამყარებს კავშირს სხვა კომპიუტერთან, როგორც წესი სერვერთან ხდება TCP/SYN და TCP/ACK ინფორმაციის პაკეტების გაცვლა. კომპიუტერი რომელიც ითხოვს კავშირს (კლიენტის ან მომხმარებლის კომპიუტერი), აგზავნის TCP/SYN პაკეტს, რომელიც უგზავნის დაკავშირების მოთხოვნას სერვერს. თუ სერვერი მზად არის კავშირის დასამყარებლად ის უგზავნის TCP/SYN-ACK პაკეტს უკან კლიენტს პასუხით „დიახ, კავშირი შესაძლებელია“, არეზერვებს ადგილს კავშირისათვის და ელოდება კლიენტის TCP/ACK პაკეტს. SYN flood-ში კლიენტის მისამართი შეცვლილია ასე, რომ სერვერი უგზავნის კლიენტს TCP/SYN-ACK პაკეტს, მაგრამ მაგისი შეტყობინება არ არის მიღებული, რადგან კლიენტი არ არსებობს ან არ ელოდება რაიმე შეტყობინებას და უგულებელყოფს გამოგზავნილ პაკეტს. ეს ტოვებს სერვერს მკვდარი კავშირით, რომელიც დარეზერვებულია კლიენტის პასუხისთვის, რომელიც თავის

მხრივ არასდროს არ მოვა. როგორც წესი, ეს ოპერაცია გამოყენებულია ბევრჯერ იმისათვის, რომ სერვერმა დაარეზერვოს ადგილი ყველა ამ კავშირისათვის და როდესაც არ დარჩება ადგილი კავშირის რეზერვირებისათვის, ლეგიტიმური კლიენტები ვერ დაამყარებენ ახალ კავშირებს.

**Exploit შეტევა** - ამ შეტევის დროს ჰაკერმა იცის უსაფრთხოების პრობლემის შესახებ ოპერაციულ სისტემაში ან პროგრამული უზრუნველყოფაში და ამ პრობლემის გამოყენებით ტეხავს სისტემას.

**Trojan ტროიანები** - ეს პროგრამები გამოიყურება, როგორც ჩვეულებრივი პროგრამული უზრუნველყოფა, მაგრამ რეალურად ასრულებენ გაუთვალისწინებელ ან თავდამსხმელის ქმედებებს გაშვების დროს. დისტანციური მართვის spyware პროგრამები ძირითადად ამ ტიპის არიან. trojan გამოყენების ტექნიკების რაოდენობა შეზღუდულია მხოლოდ თავდამსხმელის ფანტაზიით. დაინფირებული ფაილი ჩანს, იგივე ზომის როგორც რეალური ფაილი. ერთადერთი ეფექტური დაცვა არის კრიპტოგრაფიული ჯამის ან ორობითი ციფრული ხელმოწერის დროული გამოყენება.

**Bruteforce Attack პაროლიანი შეტევა**- ამ შეტევის დროს ჰაკერი ცდილობს პაროლების გატეხვას, რომლებიც შენახულია ქსელის მომხმარებლების მონაცემთა ბაზაში ან დაპაროლებულ ფაილში. არსებობს ამ შეტევის სამი ძირითადი ტიპი: ლექსიკონიანი შეტევა, brute-force შეტევა და ჰიბრიდული შეტევა. ლექსიკონიანი შეტევა იყენებს სიტყვების სია ფაილს, რომელშიც ჩაწერილია სავარაუდო პაროლები. Brute-force შეტევის დროს ჰაკერი ცდილობს ყველა შესაძლო სიმბოლოს კომბინაციით იპოვოს სწორი პაროლი.

**SQL injection ინექციის შეშვება** - injection-ს დროს ჰაკერი სვამს კოდს სერვერის მონაცემთა ბაზის SQL მოთხოვნაში. კოდი აფუჭებს საიტის რაიმე ველს, რომლის მონაცემები ჩაწერილი უნდა იყოს ბაზაში. წარმატებულ SQL injection-ს შეუძლია წაიკითხოს მნიშვნელოვანი ინფორმაცია მონაცემთა ბაზიდან, შეცვალოს ბაზის მონაცემები, შეასრულოს ადმინისტრაციული ოპერაციები მონაცემთა ბაზაზე (მაგალითად DBMS-ის გათიშვა), გაიგოს DBMS ფაილური სისტემის ფაილების შინაარსი და ზოგიერთ შემთხვევაში

**Key Logging** ქეი ლოგინგი ამ მეთოდის დროს პროგრამა მითითებულ ფაილში, ჰოსტსა თუ სერვერზე ინახავს კლავიატურაზე აკრეფილ ყველა კომბინაციას რაც იკრიფება მსხვერპლის კომპიუტერზე და დაყენებულია მალულად შემტევის მიერ, რომელიც რთულად მისაგნებია.

## 2.2. პერსონალური ინფორმაცია

ჩვენი პერსონალური ინფორმაცია კომპიუტერულ მოწყობილობის გამოყენების დროს ყველგან ფიქსირდება.

მსოფლიოს მასშტაბით ეს ბევრისთვის პრობლემაა, რომ ხდება მოწყობილობის იდენტიფიცირება, ხოლო მოწყობილობიდან გამომდინარე მფლობელის ამოცნობაც და ეს ყველაფერი ბევრისთვის ასოცირდება როგორც ტოტალურ კონტროლთან და მიყურადებასთან.

პერსონალურ ინფორმაციის უსაფრთხოებასა და დაცვაზე ზრუნავენ, როგორც სამთავრობო ასევე დიდი ბიზნეს სექტორები, რომლებსაც ასევე ხვდებათ ძალიან რთული გამოწვევები და წინააღმდეგობები, რომ შეინახონ საზოგადოების პერსონალური ინფორმაცია უსაფრთხოდ და გარანტირებულად.

პერსონალურ ინფორმაციის დაცვაზე მსოფლიოს მასშტაბით საკანონმდებლო ცვლილება ყოველდღიურად მიმდინარეობს ტექნოლოგიური სფეროს განვითარების გამო, შემუშავებულია ისეთი პროტოკოლები როგორიცაა: **GDPR, COPPA, Privacy Policy** და ასე შემდეგ.

მაგალითად GDPR - General Data Protection Regulation (მონაცემთა დაცვის ზოგადი რეგულაცია) რომელიც შემუშავებულია ევროკავშირის მიერ.

COPPA სტანდარტი - Children's Online Privacy Protection Rule (ბავშვთა ონლაინ კონფიდენციალურობის დაცვის წესი) რომელიც ეხება 13 წლამდე ასაკის ბავშვებს, რომლებსაც ეკრძალებათ ისეთ საიტებზე რეგისტრაცია, რომელზეც ეს პოლიტიკა მოქმედებს.

Privacy Policy - კონფიდენციალურობის პოლიტიკა, სტანდარტული პოლიტიკა საიტებზე, რომელიც მესამე მხარეს გადასცემს მონაცემებს გარკვეულ ჩარჩოებში.

ეს ყველაფერი ბნელ ქსელში მკაცრად დარღვეულია, არ არის არანაირი პოლიტიკის პირობა და დაცვა. ბნელი ქსელის ვებ გვერდებსა და პლატფორმებზე მიმდინარეობს შესული მოწყობილობების ანალიტიკა, ინფორმაციის შეგროვება, ვინ შევიდა, რატომ, როგორ, რისთვის და ასე შემდეგ. იდენტიფიცირება ხდება შესული მოწყობილობის ეკრანის ზომის დონეზე, ანუ შესული პიროვნების სრული ინფორმაცია ავტომატურად ბნელი ქსელის პლატფორმის სერვერზე იდენტიფიცირდება და ეს პრობლემურია დღევანდელი საზოგადოებისთვის,

მართალია მომხმარებლის რეალური IP არ ფიქსირდება, ანუ ავტომატურად ბრაუზერი ტორის ქსელში სხვა დანარჩენ პროქსებს უერთდება, მაგრამ რომელ პროქსს უერთდება ეს ფიქსირდება და ილოგება ტორის სერვერებზე.

ტორის არასწორად გამოყენების შემთხვევაში შესაძლებელია დაზიანდეს პიროვნება, როგორც მორალურ-ფსიქოლოგიურად ასევე ფინანსურადაც.

სწორედ ეს ყველაფერი არის ის რაც წარმოადგენს პრობლემას, რაც ხელს უშლის პერსონალური ინფორმაციის უსაფრთხოებას, პოლიტიკის შენარჩუნებას და არღვევს წესრიგს.

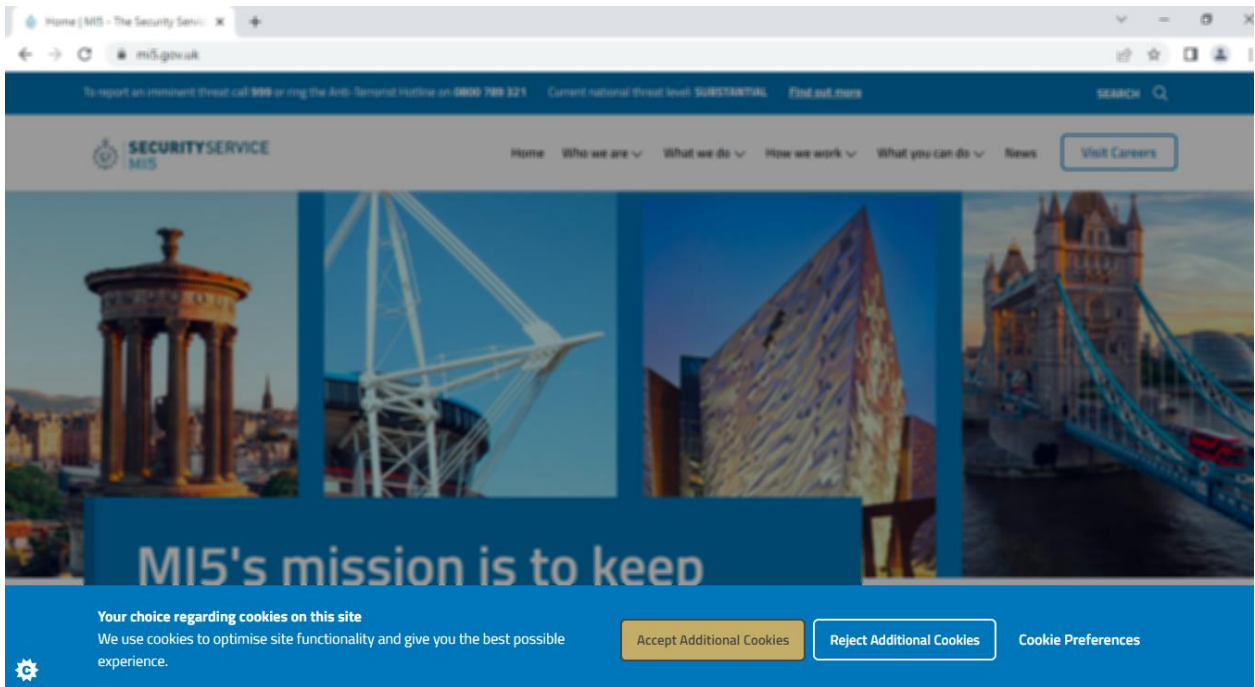
მაგრამ, აღსანიშნავია, რომ ტორის და ბნელი ქსელის განვითარებამ გამოიწვია განვითარებულიყო კიბერ შეტევის თავდაცვის მექანიზმები, პერსონალური უსაფრთხოების პოლიტიკის პირობები, მომხმარებელთა უსაფრთხოებაზე ზრუნვა და ასე შემდეგ.

მაგალითად, როდესაც ჩვენ ვიმყოფებით Surface ვებსაიტზე, ანუ საიტზე რომელსაც არ სჭირდება ტორის და მსგავსი ბრაუზერების გამოყენება, ძირითადად საიტები გვეკითხებიან რომ გამოიყენონ თუ არა ჩვენს შესახებ ინფორმაცია ანალიტიკისთვის, თუ ჩვენ მას დავეთანხმებით მაშინ ჩვენი მოწყობილობის მონაცემები დამუშავებაში გადავა და შეუერთდება სერვერზე განთავსებულ ანალიტიკურ პანელს სხვადასხვა დანიშნულებისთვის, როგორიცაა: მომხმარებლებისთვის უკეთესად მოწესრიგება

პლატფორმის მოხმარებისას, საძიებო სისტემებში მარტივად მოგნება, საიტზე რუკის ოპტიმიზაცია და ასე შემდეგ.

მაგრამ თუ ჩვენ არ დავეთანხმებით საიტზე არსებულ კითხვას, მაშინ მოწყობილობის შესახებ ინფორმაციას არ წაიღებს პლატფორმა, ანუ საიტზე შესული მოწყობილობა არ ჩაერთვება ავტომატურად სხვადასხვა საორიენტაციო ანალიტიკურ გამოთვლების სისტემებში, არ დაილოგება მიახლოებითი საიტები, მოქმედებები, კლიკები და ასე შემდეგ.

ამ ყველაფერთან ერთად საიტები, რომლებიც მკაცრად ზრუნავენ მომხმარებელთა პერსონალურ ინფორმაციაზე, შესულ ვიზიტორებს აფრთხილებენ საიტზე შესვლისთანავე, მაგალითად :



თუ ჩვენ საიტზე შევალთ, პირველ რიგში ვიხილავთ კითხვას, რომ ვეთანხმებით თუ არა რომ ჩვენი Cookies ანუ ჩვენი მოქმედებები შეინახოს სერვერზე და გადავიდეს ანალიტიკურ ველში, ხოლო თუ ჩვენ არ დავეთანხმებით მათ შემოთავაზებას არაფერი მოხდება, უბრალოდ გავაგრძელებთ საიტის გამოყენებას, ჩვენი მოქმედება არ



დაფიქსირდება საიტზე, ჩვენი დატა არ შეინახება გამუდმებით, უბრალოდ ანალიტიკურ ველში არ ჩავარდება ჩვენს მიერ შესრულებული მოქმედება.

ეს წარმოადგენს დღევანდებლობაში ერთ-ერთ საინტერესო ტექნოლოგიას, რაზე დაყრდნობითაც მუშაობენ ციფრული მარკეტერები, ანუ პერსონალური ინფორმაციის შეგროვებული ანალიტიკით მიმდინარეობს მიზანმიმართული რეკლამების მიწოდება საზოგადოებაზე და რა თქმა უნდა ყველაფერი პიროვნების ნებართვის შემდეგ, განსხვავებით ბნელი ქსელისა, სადაც ეს ყველაფერი არანაირად არ კონტროლდება და ფიზიკურად ვერც გაკონტროლდება.

პერსონალური ინფორმაციის გამოყენება ბნელი ქსელის საიტებზე უნებართვოდ გამუდმებით მიმდინარეობს, რადგან ვერცერთი რეგულაცია და ვერცერთი კანონი ვერ ებრძვის ბნელი ქსელის უზარმაზარ სისტემას.

ბნელ ქსელში მყოფი საზოგადოების ნაწილი ამ ყველაფერს მკაფიოდ აანალიზებს და სწორედ ამიტომ მიმართავენ სხვადასხვა თავდაცვის მექანიზმებს და საშუალებებს, რომ არ მოხდეს მათი იდენტიფიცირება ბოლომდე ან კვალი აურიონ მათ წინააღმდეგ დაინტერესებულ სუბიექტს.

ასევე პერსონალური ინფორმაციას კომპანიებში მიეცა ბიზნესის მხარე, ანუ მსოფლიოს მასშტაბით სხვადასხვა სოციალური ქსელები ჰყიდიან ხალხის ინფორმაციებს რაღაც სარგებლის გამო, ეს სარგებელი შეიძლება იყოს, გარიგება, ფინანსური და ასე შემდეგ.

მაგალითი რომ ვთქვათ, მსოფლიოში ერთ-ერთი ყველაზე დიდი სოციალური ქსელი Facebook-ს უკვე გადახდილი აქვს რამდენიმე მილიარდის ჯარიმები, იმის გამო, რომ კომპანიებს მიჰყიდა მომხმარებელთა ინფორმაცია, როგორიცაა ინტერესების სფერო, საკონტაქტო დეტალები, სახელი, გვარი და ასე შემდეგ.

## 2.3. პრობლემის აღმოფხვრა

ზემოთ აღნიშნული ველებიდან ჩვენ შეგვიძლია გამოვიტანოთ დასკვნა, რომ პრობლემა იმაზე უფრო მწვავეა ვიდრე ერთი შეხედვით ჩანს, ბნელი ქსელის პლატფორმებზე, ეს შეიძლება იყოს, როგორც: ინტერნეტ ფორუმი, საიტი, ბლოგი.

ირღვევა პერსონალური ინფორმაციის გამოყენების პოლიტიკა, სწორედ ამიტომ საზოგადოება არ დაეხმაროს ბნელ ქსელს განვითარებაში და არ უნდა ისარგებლოს მსგავსი პლატფორმებით ან თუ ისარგებლებენ უნდა იყოს ჩამოწერილი ყველა ის წინაპირობა რაც მოჰყვება მათ ქმედებებს ან რეკომენდაცია როგორც ვიყოთ უსაფრთხოთ “ბნელ ქსელში მოგზაურობის” პერიოდში.

სწორედ ამ პრობლემის აღმოსაფხვრელად, მარტივად ხილულ სივრცეში ანუ Surface გარემოში, სადაც ჩვენ ყოველდღიურად გვიწევს შესვლა ინტერნეტ სივრცეში წარმოგიდგენთ წამოწყებულ პროექტს და სდასუ-ს საბაკალავრო ნაშრომისთვის შექმნილ პლატფორმას ინტერნეტ ფორუმს, რომელსაც არ სჭირდება ტორის ბრაუზერი, ბნელი ქსელი და რაც მთავარია დაცულია ყველანაირად მომხმარებელთა, სტუმართა და საზოგადოების პერსონალური მონაცემები.

ასევე პრობლემის თავიდან ასაცილებლად და პერსონალური ინფორმაციის გაჟონვის წინააღმდეგ აღსაკვეთად, საჭიროა იყოს დაცული სერვერები და ჰოსტინგები, უნდა იყოს გაწერილი წესები რის მიხედვითაც მოხდება სერვერებზე და მონაცემთა ბაზებზე ადმინისტრატორის შესვლის პრივილეგიები, მაგალითად:

სერვერზე უნდა იყოს გაწერილი თეთრ სიაში შესული აიპი მისამართები, და მხოლოდ ამ კონკრეტულ აიპი მისამართებს ჰქონდეს უფლება შევიდნენ სერვერზე.

მონაცემთა ბაზებზე წვდომა უნდა შეიძლებოდეს მხოლოდ ლოკალური წყაროთი, ანუ მოწყობილობა თუ არ შევა კონკრეტული აიპი მისამართით სერვერზე, ის სხვანაირად ვერ უნდა უკავშირდებოდეს მონაცემთა ბაზას, რომელიც განთავსებულია სერვერზე.

უნდა მიმდინარეობდეს სერვერებზე განახლებების დაყენებები და სისტემური ადმინისტრატორების, ქსელის ადმინისტრატორები, დევოპს ინჟინრების, პროგრამისტების

და მოკლედ აიტი კადრის ხშირი მონიტორინგი და ტრენინგები კიბერ უსაფრთხოებაში გასაღრმავებლად და კომპეტენციის ასამაღლებლად.

შესაბამისად, თუ იქნება შექმნილი და ჩამოყალიბებული კომპანიაში უსაფრთხოების პროტოკოლი და გარკვეული რეგულაცია, მაშინ კომპანია თავიდან აიცილებს მსგავს შემთხვევებს, როგორცაა მონაცემთა ბაზების გაჟონვა, კიბერშეტევები, თავდასხმების გამკლავება და პერსონალური ინფორმაციის დაკარგვა ან დაბლოკვა.

უნდა დაიგეგმოს და შეიქმნას რეგულაციები, რომლის დაკმაყოფილების გარეშეც ვებ-გვერდები უნდა იზოლირდნენ ინტერნეტ სივრცეში, ხდებოდეს მათი მონიტორინგი და შემოწმება სხვადასხვა სტანდარტებით.

მაგალითად კომპანიას შეიძლება ჰქონდეს SIEM, DLP, Antivirus, WAF და სხვადასხვა უსაფრთხოების პროტოკოლები კომპანიაში, მაგრამ მონაცემთა ბაზაზე წვდომა გლობალური ქსელიდან არ უნდა ხორციელდებოდეს... სწორედ ამ სტილის მიდგომამ ბევრი კომპანია აზარალა და დაიკარგა მონაცემები.

ამჟამად არის საერთაშორისო სერტიფიკატები, რომლის მფლობელი კომპანიებიც ზრუნავენ პერსონალური მონაცემის უსაფრთხოებაზე, მაგრამ არ არის მითითებული კონკრეტულად საიდან შეიძლება იყოს დაშვება ამა თუ იმ პერსონალური მონაცემის ბაზებზე, როგორც ლოკალური ასევე გლობალური ქსელიდან.

ინფორმაციის გაჟონვის თავიდან ასაცილებლად დიდი კომპანიებს ძალიან კარგი მექანიზმები აქვთ შემუშავებული, რომელიც უნდა დაინერგოს ყველა სექტორში და სწორედ ამ მეთოდით შეჩერდება ინფორმაციების გაჟონვა გარედან თუ შიგნიდან არ მოხდა ხელოვნურად.

ხოლო რაც შეეხება დაცვის მექანიზმს შემდეგია: კომპანია იღებს საიტს და ერთ სერვერზე დგება ეს საიტი, ამის უკან მყოფი მონაცემთა ბაზა დგება სხვა საიტზე, კავშირი საიტს და მონაცემთა ბაზა შორის დაშიფრულია VPN კავშირით, რომლის მონაცემებიც რამდენიმე ადამიანს აქვს უსაფრთხოებისთვის.

საიტის ადმინ პანელში შესვლის გატეხვის თავის ასაცილებლად, რამდენიმე პროტოკოლია დაყენებული, როგორცაა 2 ეტაპიანი აუთენტიფიკაცია, გუგლის ქაფჩა ან მეილ დადასტურება.

საიტის ადმინ პანელზე თუ გაბრუტვის მეთოდით მოხდა შეტევა, მაშინ პლატფორმა ბლოკავს მესამე რეჟესტის მერე შემსვლელს და ეს ყველაფერი არის საიტის დაცვა.

ხოლო რაც შეეხება სერვერის და მონაცემთა მხარის დაცვის, სტრუქტურა შემდეგშია. სერვერზე დგება ფაერვოლის გაწერილი პლატფორმები, რომლებიც ბლოკავენ როგორც ბრუტფორსს ასევე დოს შეტევებსაც და რემოუთ კონექშენების მცდელობებს.

სერვერზე წვდომა ხდება მხოლოდ ლოკალური ქსელიდან, სადაც VPN კავშირი შუამავალია სერვერს და შემსვლელს შორის.

სწორედ ესეთ დაცვა არის უმაღლესი ხარისხის დაცვა, რადგან თუ როგორმე საიტი გატეხეს რამე ექსპლოიტის მეშვეობით ჰაკერებმა, მაშინ მათ დაეკარგებათ კავშირი მონაცემთა ბაზებთან, ვერ იპოვიან და უნებართვო კავშირს ვერ აიღებენ, ხოლო თუ სერვერის გატეხვა უნდათ, მაშინ ჯერ VPN კავშირზე უნდა აიღონ წვდომა, ან ლოკალურ ქსელზე უნდა აიღონ წვდომა, რომელიმე კომპიუტერის გატეხვით ან ლოკალურ ქსელზე დაჯდომით.

## 2.4. პროექტი

შევქმენი საერთაშორისო ფორუმი Hackers [...] Ge რომელიც ატარებს შემეცნებით ხასიათს, სადისკუსიო ვებსაიტს და საკომუნიკაციო საშუალებას.

ფორუმი ძრავი MyBB-ს ღია კოდზეა აგებული და ჩამენებულია ყველა ის საჭირო პროტოკოლი რაც მკაფიოდ პასუხობს პერსონალური მონაცემთა დაცვის რეგულაციას. ძრავის მოკლე მიმოხილვა რომ ვთქვათ, Mybb - ზე რათქმაუნდა რამდენიმე ათეული და ასეული კაცი მუშაობდა, სწორედ ასე დაიხვეწა და ჩამოყალიბდა ეს ძრავი, ხოლო ბირთვი აწყობილია მთლიანად PHP-ის პროგრამულ ენაზე და რათქმაუნდა ეს ძრავი მსოფლიოს მასშტაბით ერთ-ერთი წამყვანია


HACKERS.GE - Cyber Community | IT Enthusiasts and Professionals | Digital World

	Dark	yo guys whatsapp	07 May 20:41
	✓ G.	hello there	08 May 18:10
	✓ "NikaLo	Social Engineering სექცია არ არის?	09 May 03:43
	g30rg14n	@ "NikaLo სოციალური ინჟინერიის კატეგორიაა	11 May 23:46

Main Menu Community   მთავარი გვერდი				Latest Posts	
Forum	Threads	Posts	Last Post	Board Statistics	
<b>About HACKERS.GE   ჩვენს შესახებ</b> Cyber Community HACKERS.GE > IT Enthusiast <b>Sub Forums:</b> <ul style="list-style-type: none"> <li>FORUM Bugs   Reports</li> </ul>	1	1	<b>Community RULES</b> 04-08-2022, 09:26 PM by FORUMRULES	Total Threads:	58
<b>CIA - Veterans Area</b> Cyber Intelligence Alliance   Restricted Area Word Wide Web Moderated By: Cyber Intelligence Alliance	-	-	-	Total Posts:	23
<b>The Lounge   Global Reviews</b> Free space	0	0	Never	Total Members:	58
				Most Online:	766

ჰაკერს.ჯი საერთაშორისო ფორუმი წარმოადგენს ერთ-ერთ ყველაზე დაცულ ინტერნეტ ფორუმს, სადაც ამჟამად თავს იყრის ინფორმაციული ტექნოლოგიებით დაინტერესებული საზოგადოება, მიმდინარეობს ინფორმაციული მიმოცვლა და სხვადასხვა დისკუსიები სხვადასხვა საკითხებზე, რომლის მიზანიც იქნება ქართული აიტი ქომუნიტის გასვლა საერთაშორისო ასპარეზზე და ინტერნაციონალური აიტი საზოგადოების იდეების განხილვა.

საიტზე რეგისტრაციის პერიოდში, მაქვს მითითებული COPPA - ს პროტოკოლი



[Portal](#)
[Help](#)

Hello There, Guest!
 [Login](#)
[Register](#)

HACKERS.GE - Cyber Community | IT Enthusiasts and Professionals | Digital World
 [Register](#)

HACKERS.GE - Cyber Community | IT Enthusiasts and Professionals | Digital World - COPPA Compliance

In order to register on these forums, we require you to verify your age to comply with COPPA. Please enter your date of birth below.

Date of Birth:

Day:

Month:

Year:










You can choose to hide your date of birth and age by editing your profile after registering.

[Continue with Registration](#)

Lite (Archive) Mode
 [RSS Syndication](#)

Default
 [Go](#)

Powered By HACKERS, © 2022.
 

ანუ თუ მომხმარებელი ასაკში მიუთითებს რომ არ არის 13 წელზე ზემოთ, მაშინ სისტემა ავტომატურად დაბლოკავს მას და ვერ გაივლის რეგისტრაციას, ხოლო 13 წლის მოზარდებს ძირითადად არ აქვთ ინფორმაცია COPPA -ს სტანდარტებსა და რეგულაციებზე.

შემდეგი ეტაპი, უკვე საიტზე არსებული რეგულაციების და წესების დათანხმებაა

First of all, the administration of the forum HACKERS[.]GE is not responsible for the material posted on our site, as well as for the quality and results of the material uploaded by another person.

☒ This is why we recommend using a VPN or VPS network connection and virtual space such as VirtualBox, VMware and so on.

The material posted on the forum is of cognitive and educational nature.

☒ Misuse of the material posted here will remind you that it is punishable under criminal or administrative law.

The administration of the forum tries to follow the rules of the international digital space, such as: GDPR, COPPA and Privacy Policy.

The administration of the forum will delete as soon as possible the content that is related to unauthorized advertising or harms a third party. Good luck HACKERS.GE administration

---

**GEORGIAN:**

მადლობა, რომ იმყოფებით აქ ❤ იმედია იპოვით თქვენთვის სასურველ მასალას და კონტენტს.

პირველ რიგში ფორუმის ადმინისტრაცია HACKERS[.]GE იხსნის პასუხისმგებლობას ჩვენს საიტზე განთავსებულ მასალაზე, ასევე მეორე პირის ატვირთული მასალის ხარისხსა და შედეგებზე.

☒ სწორედ ამიტომ, ჩვენი რეკომენდაციაა ისარგებლოთ VPN ან VPS ქსელური კავშირით და ვირტუალური სივრცით, როგორცაა VirtualBox, VMware და ასე შემდეგ.

ფორუმზე განთავსებული მასალა ატარებს შემცენებით და სასწავლო ხასიათს.

☒ აქ განთავსებული მასალის ზოროტად გამოყენება შეგაჩვენებთ, რომ ისჯება სისხლის ან ადმინისტრაციული სამართლის კანონმდებლობით.

ფორუმის ადმინისტრაცია ცდილობს დაიცვას საერთაშორისო ციფრული სივრცის წესები, როგორცაა: GDPR, COPPA და Privacy Policy.

ფორუმის ადმინისტრაცია შეძლებისთანავე წაშლის იმ კონტენტს, რომელიც ეხება უნებართვო რეკლამირებას ან ზიანს აყენებს მესამე პირს

☐ I have read and accept the privacy policy and agreement statement.

ანუ მომხმარებელი, რომელიც საიტზე არსებულ წესებს და პირობებს არ ეთანხმება ის ვერ დარეგისტრირდება საიტზე, რა თქმა უნდა საიტზე მაქვს გაწერილი ყველაფერი ის რაც ჩაშენებულია საიტზე და რამდენად არის დაცული მომხმარებელთა პერსონალური ინფორმაცია.

ხოლო ამ ყველაფრის მერე იწყება რეგისტრაციის ველი, სადაც უნდა შეიყვანოს მისთვის საჭირო ზედმეტსახელი, ელ-ფოსტა და აქვს უფლება გამოიწეროს ან გამოწერა გააუქმოს მეილზე განახლებადი სიახლეების.

Registration

Account Details

Username:

Password:

Confirm Password:

Email:


Confirm Email:

Referrer:

If you were referred by another member you can enter their username below. If not, simply leave this field blank.

Image Verification

Please enter the text contained within the image into the text box below it. This process is used to prevent automated spam bots.

  
(case insensitive)

Account Preferences:

☒ Receive emails from the Administrators.  
☐ Hide your email from other members.  
☒ Receive private messages from other users.  
☒ Alert me with a notice when I receive a Private Message.  
☐ Notify me by email when I receive a new Private Message.  
☐ Hide me from the Who's Online list.  
Default Thread Subscription Mode:

Time Zone (DST correction excluded):

If you live in a time zone which differs to what this board is set at, you can select it from the list below.

Daylight Saving Time correction:

ასევე ფიქსირებულია, რომ რეგისტრაციის გავლის მერე, საიტზე მყოფი მოდერატორები ამტკიცებენ მომხმარებლებს.

აღსანიშნავია, რომ საიტზე დანიშნული ყველა მოდერატორი, ედიტორი თუ ადმინისტრატორი დიდი სანდოობით სარგებლობს მთავარ ადმინისტრატორთან, მთავარი ადმინისტრატორი არ ერთვება რეგისტრაციის ყოველდღიურ პროცესში, ის საიტზე უყურებს აქტივობას და კონტენტს.

რეგისტრაციის მომენტში მომხმარებელს აქვს არჩევის უფლება, სიახლეების გამოწერა მეილის მეშვეობით, ასევე მიიღოს თუ არა პირადი შეტყობინებები ფორუმზე რეგისტრაციის შემდეგ, როგორი სტატუსი მიენიჭოს მას ფორუმზე როცა ხაზზე იქნება ჩანდეს თუ არა და ასე შემდეგ.

ხოლო ეს ყველაფერი ერთად ქმნის იმ სრულფასოვან და კომფორტულ გარემოს, სადაც მომხმარებლების უფლებები დაცულია და მეგობრული სტაფიც არის.

User Maintenance
<b>Basic instructions for maintaining a forum account.</b>
<b>USER Registration</b> Registered USERS Accept forum rules
<b>Hackers.GE FORUM Rules</b> Rules for hackers.ge website internet forum
<b>Privacy Policy &amp; GDPR</b> Privacy Policy and Data Protection Rights
<b>Terms and Conditions</b> terms and conditions hackers
<b>Password RULES</b> Lost Password Recovery

ხოლო ამ ფოტოზე გამოსახულია დახმარების ველი, ანუ კატეგორია სადაც სხვადასხვა წესები წერია, როგორც მონაცემთა პერსონალური დაცვის შესახებ ასევე საიტზე მყოფი მომხმარებლების უსაფრთხოების გარანტიებად.

სწორედ მსგავსი ლოგიკით უნდა იყოს სტანდარტიზაცია, ვებ გვერდებზე რეგისტრაციის და რეგულაციის დაწესების, სადაც ბევრი საინფორმაციო გაჟონვა აღარ მოხდება და საიტზე მყოფი მომხმარებლის ინფორმაცია იქნება იმაზე უფრო დაცული ვიდრე ახლა ძალიან ბევრ საიტზე არის.

ასევე აღსანიშნავი ფაქტია, რომ ბაზა რომელიც ამ ფორუმს აქვს არის ლოკალური, ანუ გარე აიპი მისამართიდან თუ საიტი ვინმემ რამენაირად გატეხა ბაზაში ვერ შევა, ბაზა დადგმულია ლოკალურად სერვერზე, სადაც მხოლოდ სერვერზე მოხვედრის ხდება წვდომის უფლების აღება, ხოლო სერვერზე წვდომა მხოლოდ Whitelist - ში ანუ დაშვებულ აიპებში მფყოფ მოწყობილობებს აქვთ, მოკლედ რომ ვთქვათ თუ ჰაკერმა სერვერის და საიტის გატეხვასთან ერთად არ დაკლონა ჩემს მიერ დაშვებული აიპები, ის მონაცემთა ბაზაში ვერ შევა და ინფორმაციას ვერ მოიპარავს, ხოლო ამ მეთოდით მე გარანტია მაქვს რომ



ჩემს საიტზე მყოფი მომხმარებლები იქნებიან დაცულები და უსაფრთხოდ მექნება მონაცემთა ბაზა

საიტზე მყოფი მომხმარებელთა პერსონალური ინფორმაცია დაცულია და მიუწვდომელია.

MyBB

Home Configuration Forums & Posts **Users & Groups** Templates & Style Tools & Maintenance

Users & Groups

Users

**Awaiting Activation**

Groups

User Titles

Banning

Admin Permissions

Mass Mail

Group Promotions

Home > Awaiting Activation

Awaiting Activation

Here you can manage users who are awaiting activation. Please note any user who is awaiting email activation will not need to confirm their email if they are activated here.

**Manage Awaiting Activation**

	Username	Registered	Last Active	Email	IP Address	Type
<input type="checkbox"/>	აორპეფო	05-29-2022, 01:29 AM	05-29-2022, 01:30 AM	ojeyuo@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	ყოოოუეცუმ	05-29-2022, 12:06 AM	05-29-2022, 12:06 AM	ewehore@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	Mytime	05-26-2022, 09:54 PM	05-28-2022, 09:39 PM	Mytime07@protonmail.com	41.242.138.3	Awaiting Administrator Activation
<input type="checkbox"/>	იკიტეგი	05-25-2022, 01:55 AM	05-25-2022, 01:56 AM	exjorm@enau.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	elkeyefora	05-25-2022, 01:36 AM	05-25-2022, 01:36 AM	eriduj@enau.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	Kratom	05-23-2022, 12:29 PM	05-23-2022, 12:30 PM	del@freelocation.xyz	51.81.87.93	Awaiting Administrator Activation
<input type="checkbox"/>	Mauricerah	05-22-2022, 03:55 PM	05-23-2022, 07:11 PM	Zu@toncinema.online	45.87.60.42	Awaiting Administrator Activation
<input type="checkbox"/>	ბევხოუგა	05-16-2022, 03:33 AM	05-16-2022, 03:33 AM	aletnaap@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	ახობაურს	05-16-2022, 03:21 AM	05-16-2022, 03:22 AM	seqemes@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	მწკაი	05-16-2022, 03:10 AM	05-16-2022, 03:11 AM	ibobex@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	იახივბო	05-10-2022, 09:24 PM	05-10-2022, 09:24 PM	izulu@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	იაკოუაჟუ	05-10-2022, 09:15 PM	05-10-2022, 09:15 PM	ohigufale@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	ევაქეჟი	05-06-2022, 11:14 PM	05-06-2022, 11:16 PM	oeqebbx@enau.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	enapafama	05-06-2022, 10:35 PM	05-06-2022, 10:36 PM	idsjul@enau.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	montgagela	05-04-2022, 07:44 AM	05-04-2022, 07:44 AM	kelsy@electriccoter.town	147.124.223.96	Awaiting Administrator Activation
<input type="checkbox"/>	Temortage	05-04-2022, 12:53 AM	05-04-2022, 12:53 AM	terrell@lanme.creditcard	176.125.230.26	Awaiting Administrator Activation
<input type="checkbox"/>	kzmortage	05-03-2022, 11:22 PM	05-03-2022, 11:23 PM	kristopher@electriccoter.town	147.124.223.96	Awaiting Administrator Activation

Activate Users Delete Users

Powered By MyBB. © 2002-2022 MyBB Group.

Generated in 25 ms with 8 queries. Memory Usage: 2 MB

მაგალითისთვის, ზემოთ მოყვანილი ფოტო არის ის გარემო, სადაც მომხმარებლები ელოდებიან მოდერატორებისგან და ედიტორებისგან აქტივაციის დადასტურებას.

	Username	Registered	Last Active	Email	IP Address	Type
<input type="checkbox"/>	აორპეფო	05-29-2022, 01:29 AM	05-29-2022, 01:30 AM	ojeyuo@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	ყოოოუეცუმ	05-29-2022, 12:06 AM	05-29-2022, 12:06 AM	ewehore@ideaj.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation
<input type="checkbox"/>	Mytime	05-26-2022, 09:54 PM	05-28-2022, 09:39 PM	Mytime07@protonmail.com	41.242.138.3	Awaiting Administrator Activation
<input type="checkbox"/>	იკიტეგი	05-25-2022, 01:55 AM	05-25-2022, 01:56 AM	exjorm@enau.fodiscmail.com	54.39.50.123	Awaiting Administrator Activation

აქ გარკვევით ჩანს სახელები და აიპები, ანუ ეს პოტენციური სკამერები არიან, რომლებიც იტყუებიან ან ხალხს ატყუებენ გარკვეული სარგებლის სანაცვლოდ, ამიტომ ამათი რეგისტრაცია ფორუმზე არ დაიშვება და ისინი იმყოფებიან საკარანტინო ზონაში, საიდანაც მოხდება მათი აიპების სკამერების ბაზებში შეყვანა და შემდეგ დაბლოკვა.

## დასკვნა

დაკსვნის სახით შეგვიძლია, ვთქვათ რომ პერსონალური ინფორმაცია ბნელ ქსელში არაა დაცული, მიმდინარეობს ყველა მოწყობილობის მაქსიმალური მონიტორინგი და შავი საიტების რეკლამირება, რომლებიც ჰყიდიან საზოგადოების პირად ინფორმაციებს ხოლო ამ ყველაფერს აგროვებენ სწორედაც, რომ ბნელი ქსელის მეშვეობით, სადაც ჩართულია უამრავი ფორუმი, მარკეტი, საიტი, პლატფორმა და ასე შემდეგ.

თუ პიროვნება არ ერკვევა სათანადოდ ბნელ ქსელში და მასში არსებულ მიმდინარე ვითარებაში, მისთვისვე უკეთესი იქნება არ ისარგებლოს იქ, არ დაათვალიეროს და არ შევიდეს არც ერთ ქსელზე, რადგან ასე ის ყველანაირ პრობლემას თავს აარიდებს.

ბნელი ქსელი ყოველდღიურად იზრდება, იქმნება ახალი ფორუმები და ახალი საზოგადოება, ჩნდება ახალი დანაშაულის მექანიზმები და მეთოდები, როგორიცაა: კარტებით, ხალხით, ნარკოტიკებით და იარაღებით ვაჭრობა, ამიტომ ჩვენ უნდა ვურჩიოთ ჩვენს გარშემო მყოფებს რომ არ დაინტერესდნენ ამ გარემოებით, რადგან შეიძლება ძალიან დიდი პრობლემებში გაეხვნიან, ან დაკარგან პირადი ინფორმაცია გაუცნობიერებლად.

განვითარებული სახელმწიფოები დიდი ყურადღებას აქცევენ ინფორმაციულ ტექნოლოგიებს და პერსონალურ ინფორმაციის დაცვას, სწორედაც რომ ეს ყველაფერი უფრო უნდა გაძლიერდეს და ჩატარდეს უფრო მეტი ორგანიზებული შეხვედრები, რომ დაცული იყოს თითოეული ჩვენგანის პირადი ინფორმაცია და უსაფრთხო იყოს ჩვენი ინტერნეტ სივრცეში მოღვაწეობა.

## გამოყენებული ლიტერატურა

1. <https://seclab.ge/ge/HackersTools>
  2. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
  3. <https://nulled.to>
  4. <https://blackbones.net>
- 

## შენიშვნა

ფორუმი საჩვენებელი იყო, ამჟამად დომეინზე Hackers.Ge გაშვებულია კიბერ სიახლეების საიტი, სადაც ქვეყნდება მსოფლიოს მასშტაბით ტექნოლოგიურ, კიბერ და აიტი სამყაროში მიმდინარე მოვლენები.

