ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი

როგორ დავიცვათ პირადი უსაფრთხოება Facebook-ში

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

ივლისი, 2017

შინაარსი

შესავალი 3

ზოგადი რჩევები 3

Facebook-ში შესვლა 6

აუდიტორიის მართვა 8

მონიშვნის (tag) ფუნქცია 11

პირადი მონაცემების მართვა 13

შესავალი

Facebook საქართველოში ყველაზე პოპულარული სოციალური ქსელია. ოფიციალური მონაცემებით, საქართველოში 2 მილიონზე მეტი **Facebook** ანგარიშია დარეგისტრირებული, ხოლო სოციალური ქსელების მომხმარებელთა 79% სულ მცირე კვირაში ერთხელ მაინც ამოწმებს **Facebook**-ს.

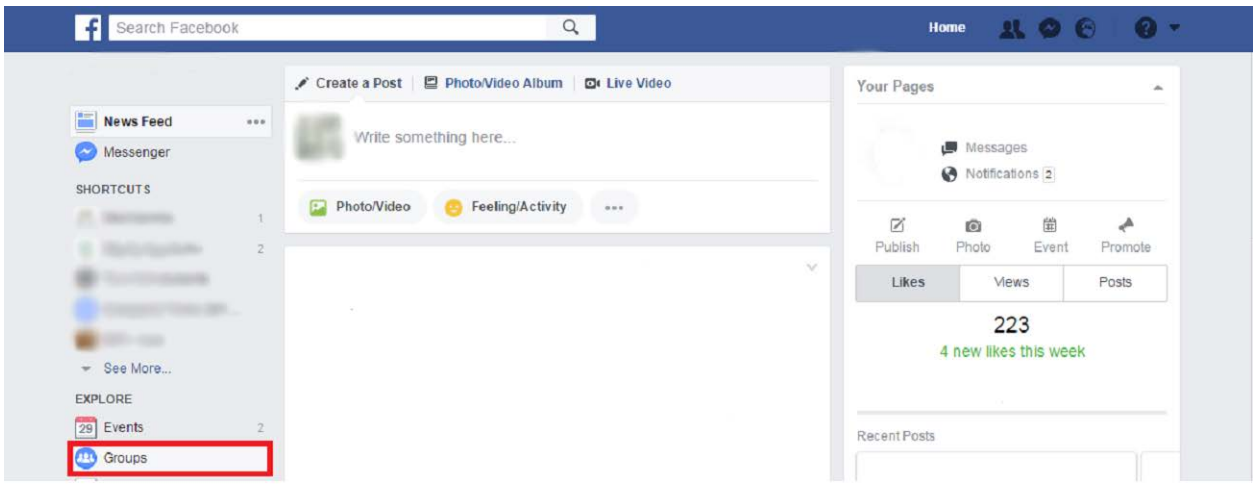
Facebook-ის მოხმარებას, სარგებლის გარდა, თან გარკვეული რისკებიც ახლავს. ბოლო მონაცემებით, 83 მილიონი ყალბი **Facebook** ანგარიში არსებობს. ასეთი ანგარიშები ხშირ შემთხვევაში იდენტობის დაფარვის ან ინფორმაციის ანონიმურად გავრცელების მიზნებით გამოიყენება. მათი არსებობა სოციალური ქსელის გამოყენების რისკს საგრძნობლად ზრდის, რადგან ყალბი ანგარიშის მფლობელს შეუძლია მარტივად მიითვისოს თქვენი იდენტობა, დაუმეგობრდეს თქვენსავე მეგობრებს და მათგან თქვენივე პირადი ინფორმაცია გამოითხოვოს.

საბედნიეროდ, **Facebook** ითვალისწინებს ამ და სხვა რისკებს და აძლევს მომხმარებელს არაერთ საშუალებას, აკონტროლოს საკუთარი უსაფრთხოების პარამეტრები. მაგალითად, **Facebook**-ზე განსაკუთრებულად მოწყვლადი სეგმენტისთვის - მოზარდებისთვის - სპეციალური უსაფრთხოების პორტალია შექმნილი. თუმცა, სამწუხაროდ, ცოტამ თუ იცის ამ საშუალებების შესახებ.

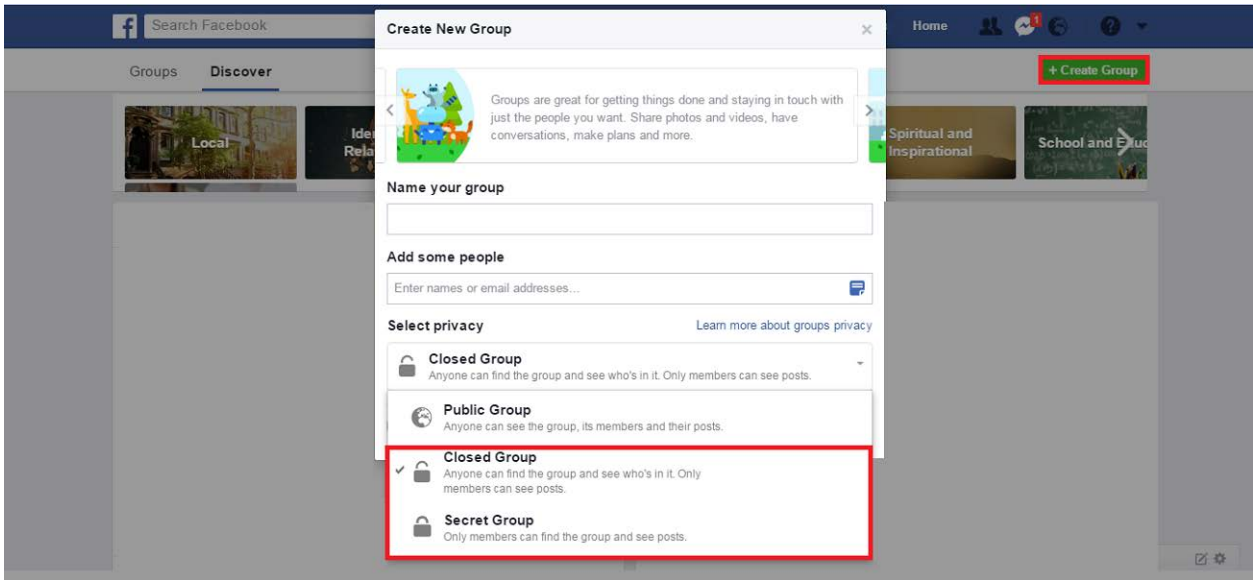
სწორედ ამიტომ, IDFI-მ მოამზადა **Facebook** უსაფრთხოების გზამკვლევი, რომელიც დაგეხმარებათ პირადი ინფორმაციის დაცვაში.

ზოგადი რჩევები

<u>**მოერიდეთ საეჭვო ჯგუფებში გაწევრიანებას**</u> - თუ ჯგუფი საეჭვო საქმიანობას ან ამგვარი საქმიანობის აგიტაციას ეწევა, ეს საკმარისი საფუძველია, არ გაწევრიანდეთ მასში. თუ თქვენ არ იცით, ვინ არის ჯგუფის ადმინისტრატორი ან ზუსტად რა მიზანი აქვს მას, ნურც ამ შემთხვევაში გაწევრიანდებით ჯგუფში. თუ თქვენ თავად მართავთ რაიმე ჯგუფს და არ გსურთ, ჯგუფის აქტივობა ყველასათვის თვალსაჩინო იყოს, აქციეთ იგი „დახურულ“ ან „საიდუმლო“ ჯგუფად. ამგვარად, ჯგუფში გავრცელებულ ინფორმაციაზე წვდომა მხოლოდ ამავე ჯგუფში გაწევრიანებულ მომხმარებლებს ექნებათ.



სურათი 1: ახალი ჯგუფის შესაქმნელად, გადადით Facebook-ის აპლიკაციების პანელში და აირჩიეთ "Groups".

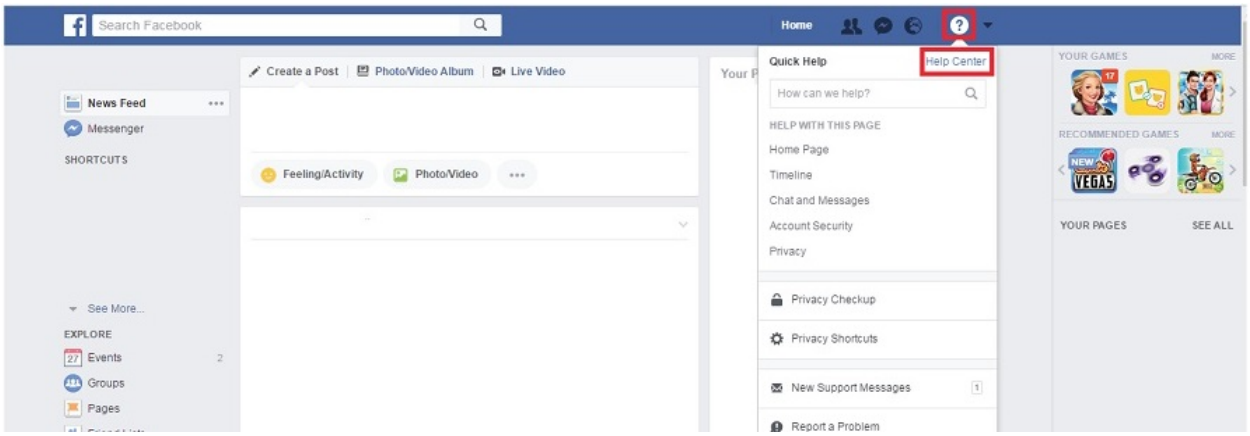


სურათი 2: აირჩიეთ "Create Group", შემდეგ კი აქციეთ იგი დახურულ ან საიდუმლო ჯგუფად.

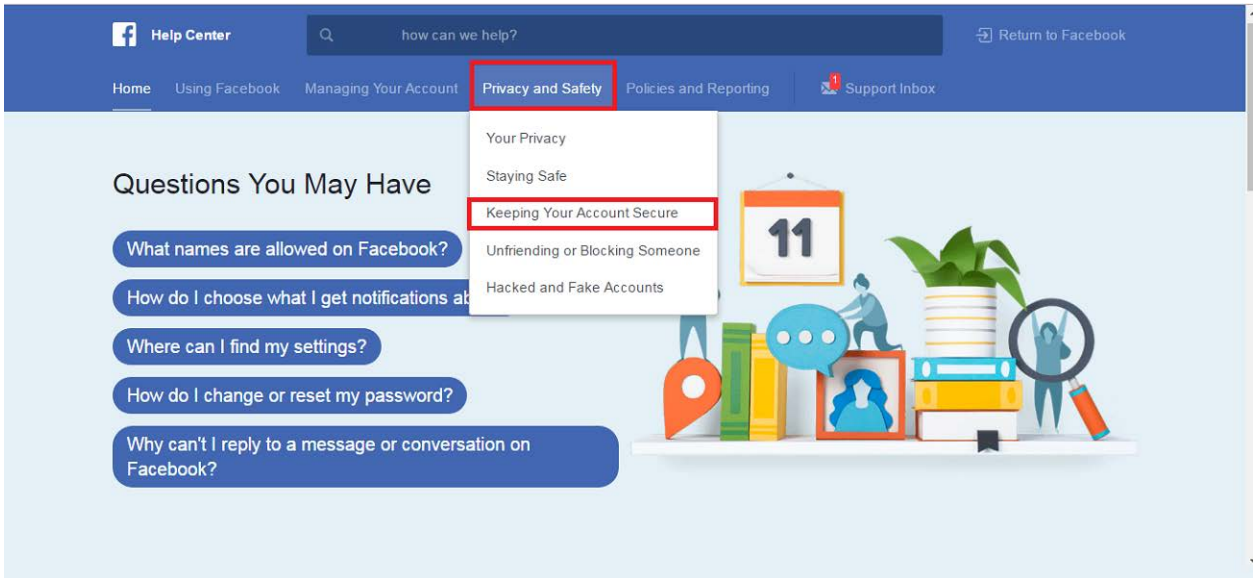
<u>მოერიდეთ უცნობი ადამიანების დამატებას მეგობრებად</u> - სავარაუდოდ, ყველას გქონიათ შემთხვევა, როდესაც სრულიად უცნობ ადამიანს გამოუგზავნია თქვენთვის მეგობრობის მოთხოვნა. ასეთ შემთხვევებში, დათანხმებამდე, შეგიძლიათ, გადაამოწმოთ, გყავთ თუ არა საერთო მეგობრები ან შეეკითხოთ მას მისი ვინაობა.

<u>მოერიდეთ საეჭვო ბმულებზე გადასვლას</u> - თუნდაც ის სანდო მეგობარმა გამოგიგზავნოთ. შესაძლებელია, რომ თქვენი მეგობრის ანგარიში გატეხილი იყოს და ავტომატურად აგზავნიდეს ვირუსის შემცველ ბმულებს. ასევე, არ გახსნათ Facebook ჯგუფებში ან გვერდებზე დადებული საეჭვო ბმულები.

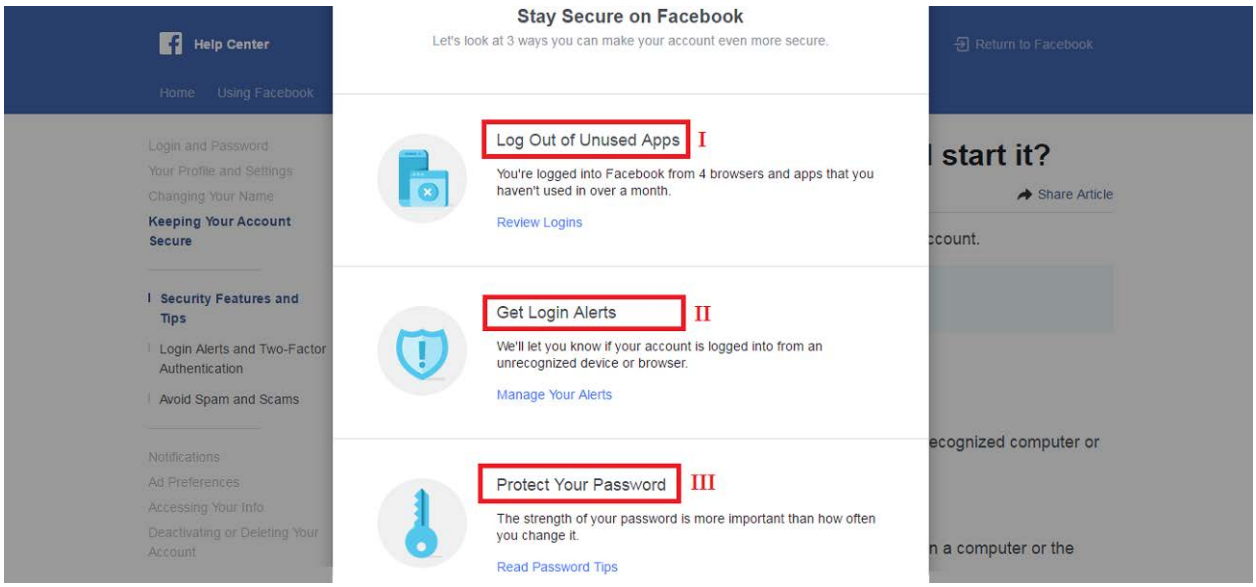
<u>**უსაფრთხოების პერიოდული შემოწმება**</u> - იმისათვის, რომ Facebook-ის მოხმარებისას თავი ბოლომდე დაცულად იგრძნოთ, რეკომენდირებულია, დროდადრო გაიაროთ ე.წ. „უსაფრთხოების შემოწმება“ (Security Checkup).



სურათი 3: უსაფრთხოების პერიოდული შემოწმების გასავლელად, Facebook-ის ზედა მარჯვენა კუთხეში არსებული მენიუს საშუალებით, აირჩიეთ "Help Center".



სურათი 4: მონიშნეთ "Privacy and Safety", შემდეგ კი - "Keeping Your Account Secure".



სურათი 5: როგორ გავააქტიურო უსაფრთხოების შემოწმება: I - შემოწმების გავლისას სისტემა ავტომატურად თიშავს თქვენი Facebook-ის ანგარიშს იმ ბრაუზერებიდან და აპლიკაციებიდან, რომლებსაც დიდი ხანია, აღარ სტუმრობთ. II - ამგვარი შემოწმება ასევე გეხმარებათ, მიიღოთ თქვენს ანგარიშზე შესვლის შესახებ შეტყობინებები. III - შემოწმება ასევე გეხმარებათ, მიიღოთ ინფორმაცია თქვენი პროლის უსაფრთხოების შესახებ.

Facebook-ში შესვლა

პროლის უსაფრთხოება - რამდენიმე მარტივი რჩევა:

- გამოიყენებთ გრძელი პროლები - არანაკლებ 8 სიმბოლო;
- პროლის შექმნისას შეეცადეთ დაეყრდნოთ სიმბოლოების შემთხვევითი შერჩევის მეთოდს;
- შეეცადეთ, პროლში გამოიყენოთ არასტანდარტული სიმბოლოები - მაგალითად, სასვენი ნიშნები;
- პერიოდულად ცვალეთ თქვენი პროლი - მაგალითად, სამ თვეში ერთხელ;
- არ გაუზიაროთ თქვენი ანგარიშის პროლი სხვა ადამიანებს.

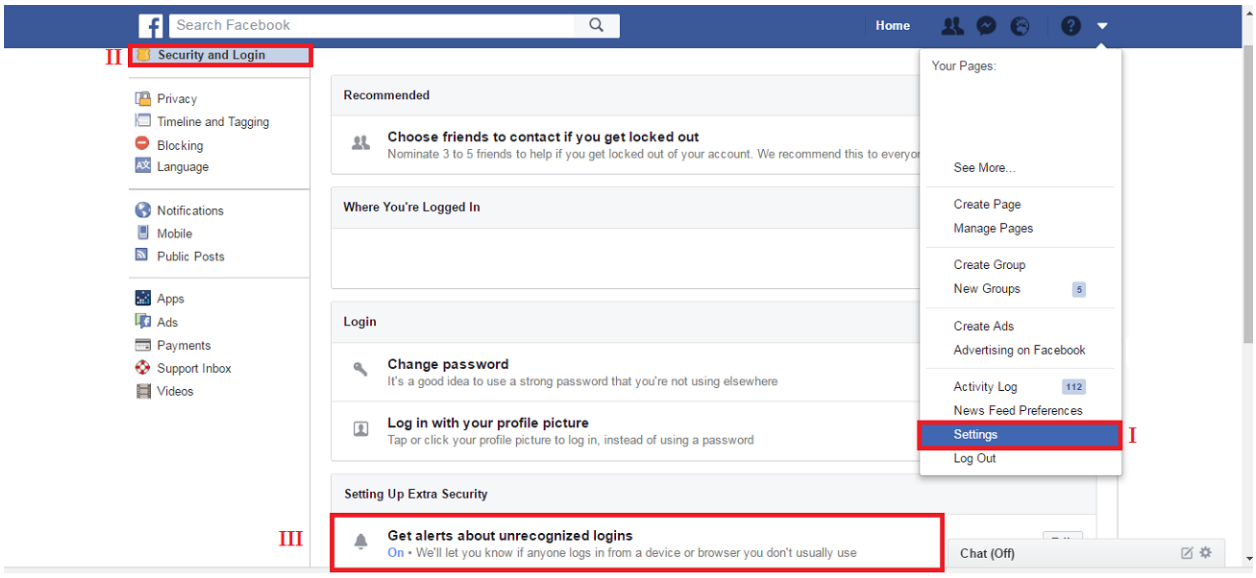
სუსტი პროლი: password

ძლიერი პროლი: “$sap_s15w*8d~

თქვენი პროლის სიძლიერის შესამოწმებლად შეგიძლიათ გამოიყენოთ: www.passwordmeter.com

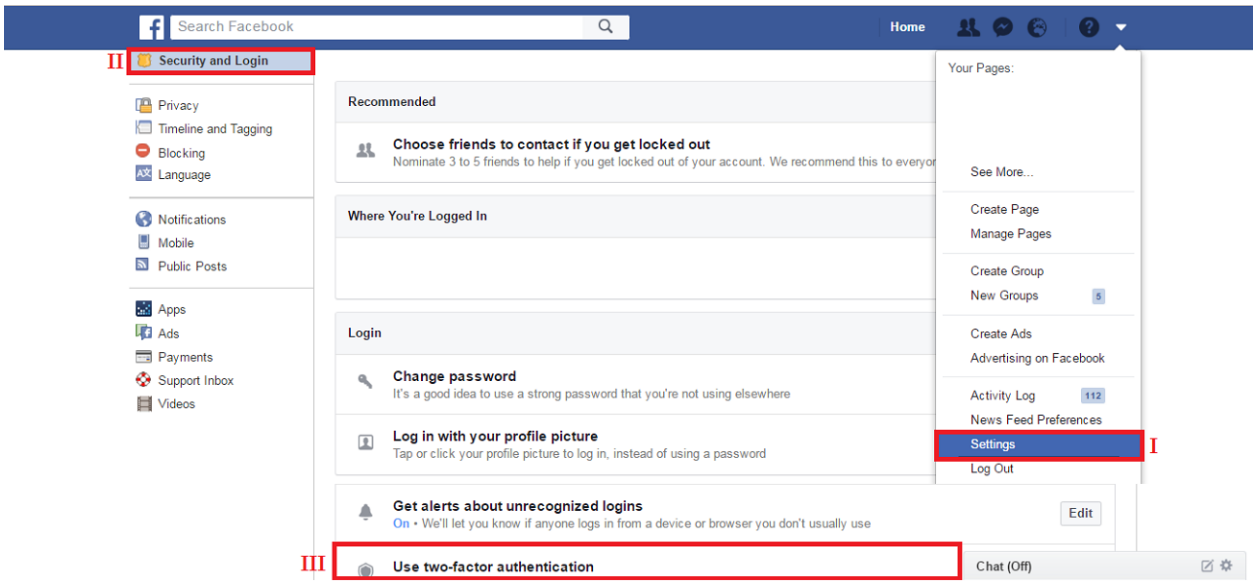
შესვლის შეტყობინება (Login Alerts) - ფუნქცია გაძლევთ საშუალებას, ელ-ფოსტაზე მიიღოთ შეტყობინება, როდესაც თქვენს Facebook ანგარიშზე ნებისმიერი ახალი მოწყობილობიდან ხდება შესვლა. ამგვარად, თქვენ იგებთ ვინ და საიდან შედის თქვენს ანგარიშზე. ზოგადად,

შეეცადეთ, Facebook-ზე არ შეხვიდეთ არასანდო კომპიუტერიდან და, რაც უფრო მნიშვნელოვანია, ასეთი მოწყობილობაზე არ დატოვოთ თქვენი ანგარიში ჩართული.



სურათი 6: როგორ გავააქტიურო შესვლის შეტყობინება: I – Facebook-ის ზედა მარჯვენა კუთხეში არსებული მენიუს საშუალებით, აირჩიეთ პარამეტრები. II - უსაფრთხოება. III - ჩართეთ შეტყობინების მიღების ფუნქცია.

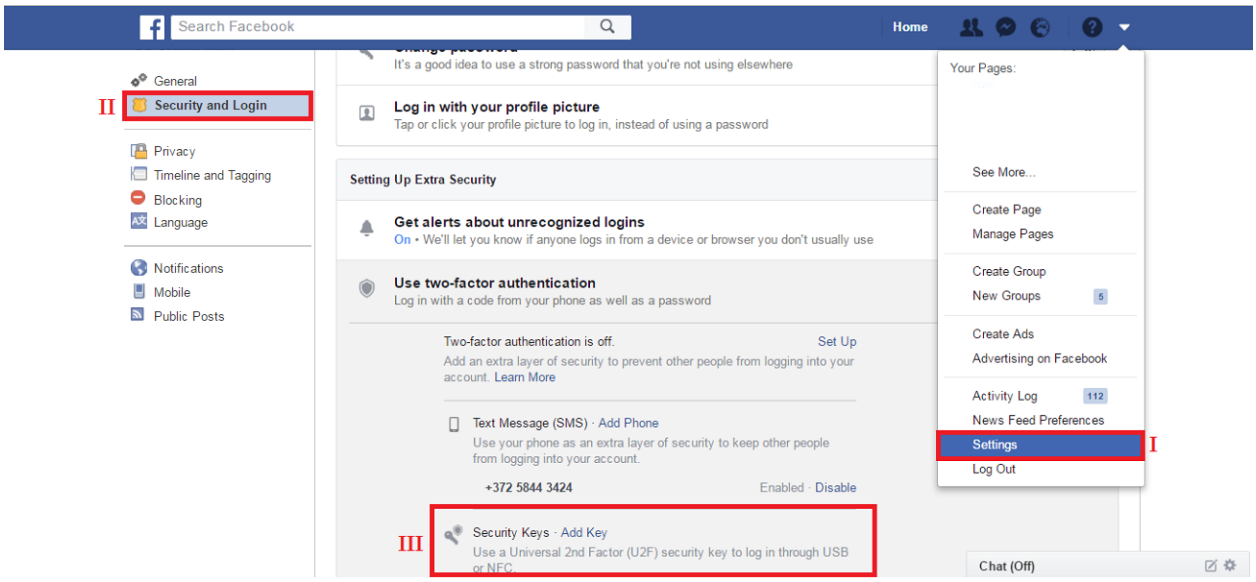
<u>2-ეტაპიანი ავტორიზაცია (Two-Factor Authentication) -</u> ფუნქციის გააქტიურების შემდეგ, მომხმარებლის სახელისა და პაროლის მოთხოვნას ემატება SMS-ით მიღებული კოდიც. SMS კოდის შეყვანა საჭირო ხდება Facebook-ში ახალი მოწყობილობიდან შესვლის დროს.



სურათი 7: როგორ გავააქტიურო <u>2 - ეტაპიანი ავტორიზაცია</u>: I – Facebook-ის ზედა მარჯვენა კუთხეში არსებული მენიუს საშუალებით, ეწვიეთ პარამეტრებს. II - უსაფრთხოება. III - ჩართეთ 2-ეტაპიანი ავტორიზაცია.

<u>უსაფრთხოების გასაღები (Security Key) -</u> საშუალებას გაძლევთ, Facebook-ის ანგარიშს დაუკავშიროთ ნებისმიერი USB ხელსაწყო, რომელიც შემდეგ, სხვა კომპიუტერიდან შესვლის დროს „გასაღების“ როლს ასრულებს. Facebook-ის გარდა, უსაფრთხოების გასაღები Google,

Dropbox და სხვა პლატფორმებისთვისაც იმუშავებს. მის გამოსაყენებლად Chrome-ის უახლესი ვერსია დაგჭირდებათ.

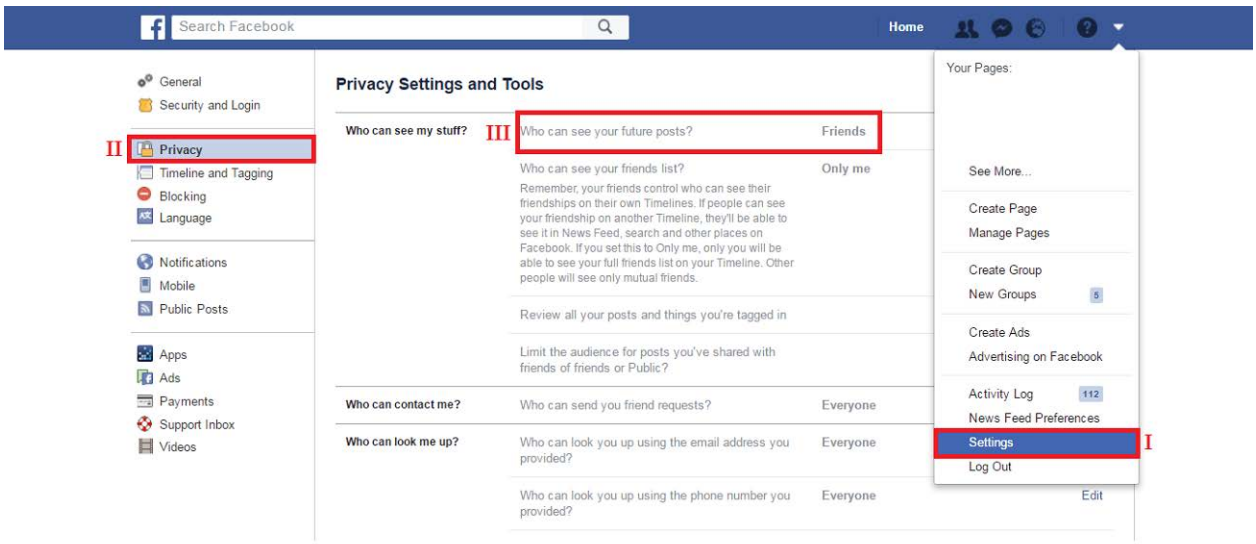


სურათი 8: როგორ გავააქტიურო <u>უსაფრთხოების გასაღები</u>: I – Facebook-ის ზედა მარჯვენა კუთხეში არსებული მენიუს საშუალებით, აირჩიეთ პარამეტრები. II - უსაფრთხოება. III - დაამატეთ გასაღები.

აუდიტორიის მართვა

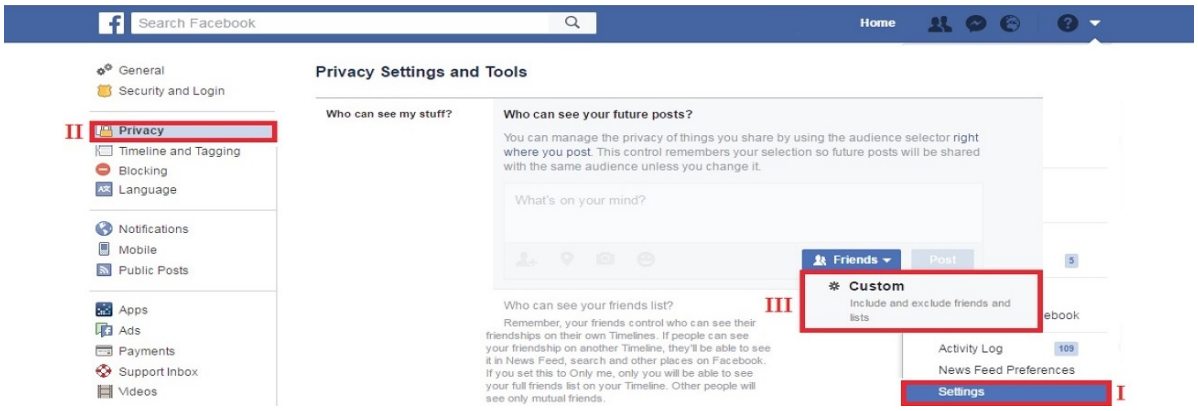
<u>აკონტროლეთ, ვის შეუძლია თქვენი პოსტების ნახვა</u>

Facebook საშუალებას გაძლევთ, აკონტროლოთ, თუ ვის შეუძლია დაინახოს თქვენ მიერ გაზიარებული ინფორმაცია - ყველას, მხოლოდ მეგობრებს, თუ თქვენი მეგობრების კიდევ უფრო ვიწრო ჯგუფს.



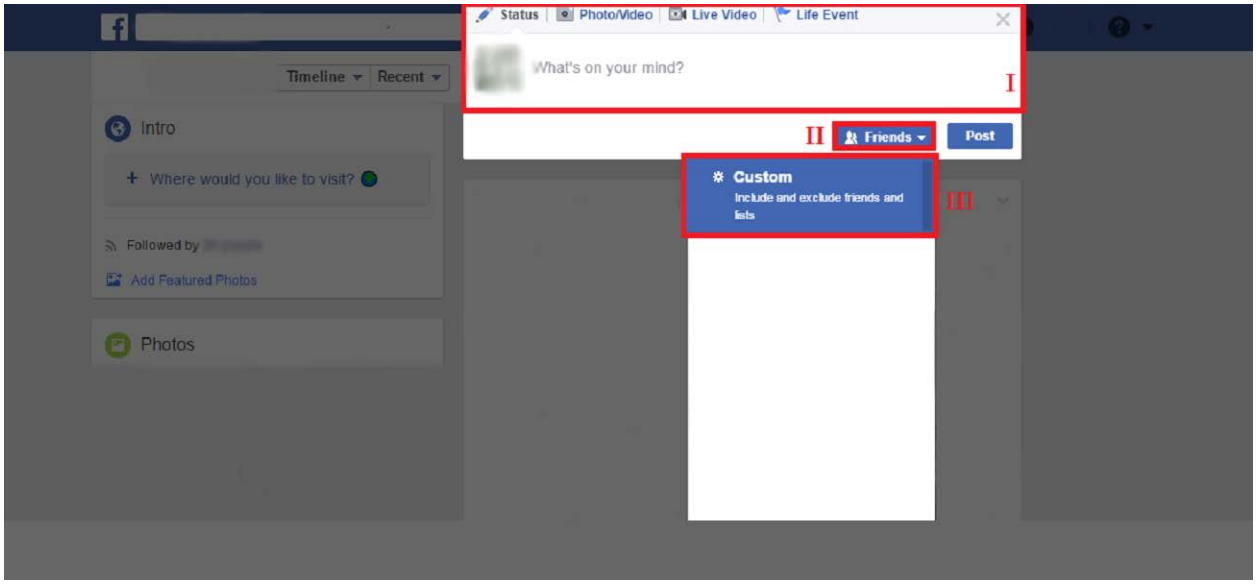
სურათი 9: აუდიტორიის მართვა: I – Facebook-ის მარჯვენა ზედა კუთხეში არსებული მენიუს საშუალებით, აირჩიეთ პარამეტრები. II - კონფიდენციალურობა. III - ვის შეუძლია ნახოს ჩემი პოსტები, შემდეგ კი - მონიშნეთ შესაბამისი აუდიტორია.

Facebook ვიწრო აუდიტორიის არჩევის საშუალებასაც გაძლევთ, რისთვისაც ე.წ სამიზნე აუდიტორიაზე უკეთ მორგებული (Custom) გაზიარების ფუნქცია უნდა გამოიყენოთ.



სურათი 10: აუდიტორიის შერჩევა: I - აირჩიეთ პარამეტრები. II - კონფიდენციალურობა. III - აირჩიეთ ვიწრო აუდიტორია, "Custom" ფუნქციის გამოყენებით.

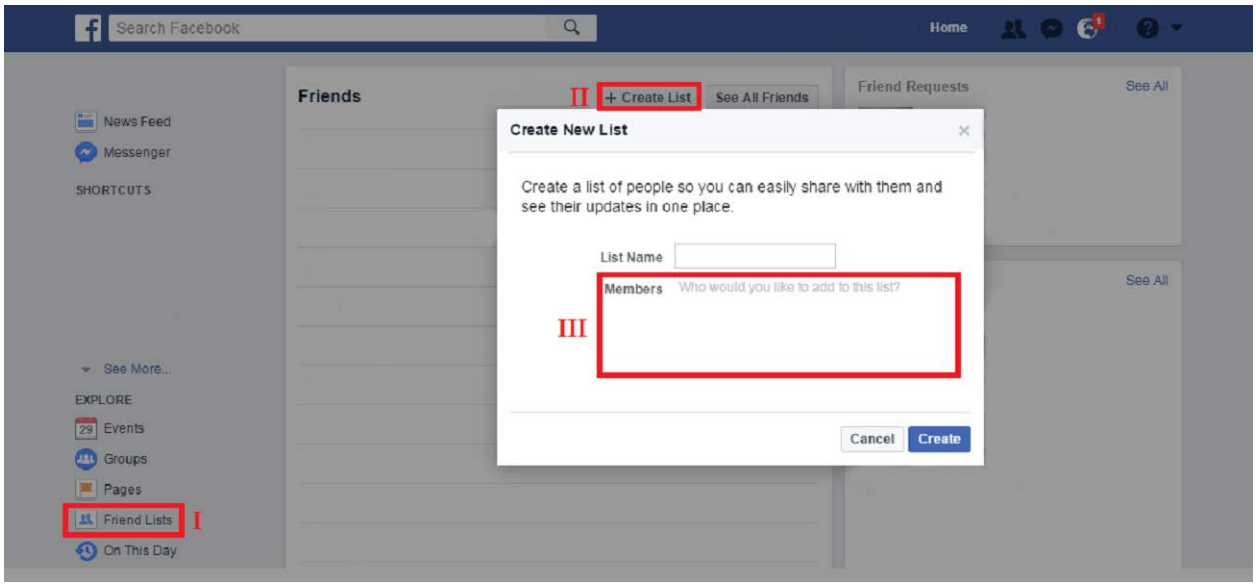
აუდიტორიის შეზღუდვა შეგიძლიათ თითოეული პოსტის შემთხვევაშიც. ამისათვის, ინფორმაციის გაზიარების მომენტში, უნდა შეცვალოთ სამიზნე აუდიტორია ისე, როგორც მომდევნო ფოტოებზეა მოცემული. ამ შემთხვევაშიც შეგიძლიათ, გამოიყენოთ „Custom" ფუნქცია და გადაწყვიტოთ, ვის გაუზიარებთ და ვის დაუმალავთ კონკრეტულ პოსტს.



სურათი 11: აუდიტორიის შეზღუდვა: I - გადადით თქვენს კედელზე. II - მონიშნეთ აქტივობის ფანჯარა. III - აირჩიეთ შესაბამისის აუდიტორია, "Custom" ფუნქციის გამოყენებით.

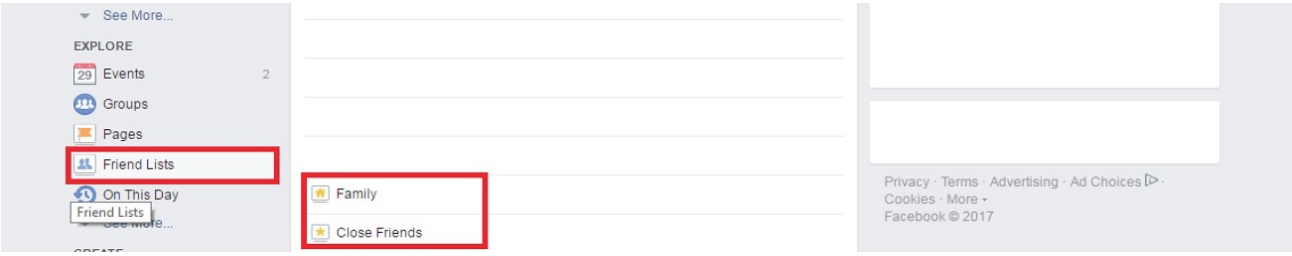
სიების შექმნა

აუდიტორიის მართვას კიდევ უფრო ამარტივებს სიების შექმნის ფუნქცია. თქვენ შეგიძლიათ, შექმნათ სამსახურის, ახლო მეგობრებისა, თუ ნათესავების სია და ნებისმიერი მასალა მხოლოდ მათ დაუმალოთ ან გაუზიაროთ.



სურათი 12: სიის შესაქმნელად: I - გადადით აპლიკაციების პანელში. II - შექმენით ახალი სია ("Create List"). III - დაამატეთ სიაში მეგობრები.

გარდა ამისა, არსებობს Facebook-ის მიერ ავტომატურად, მეგობრების პროფილიდან მიღებული ინფორმაციების მიხედვით შექმნილი „ჭკვიანი“ სიები.

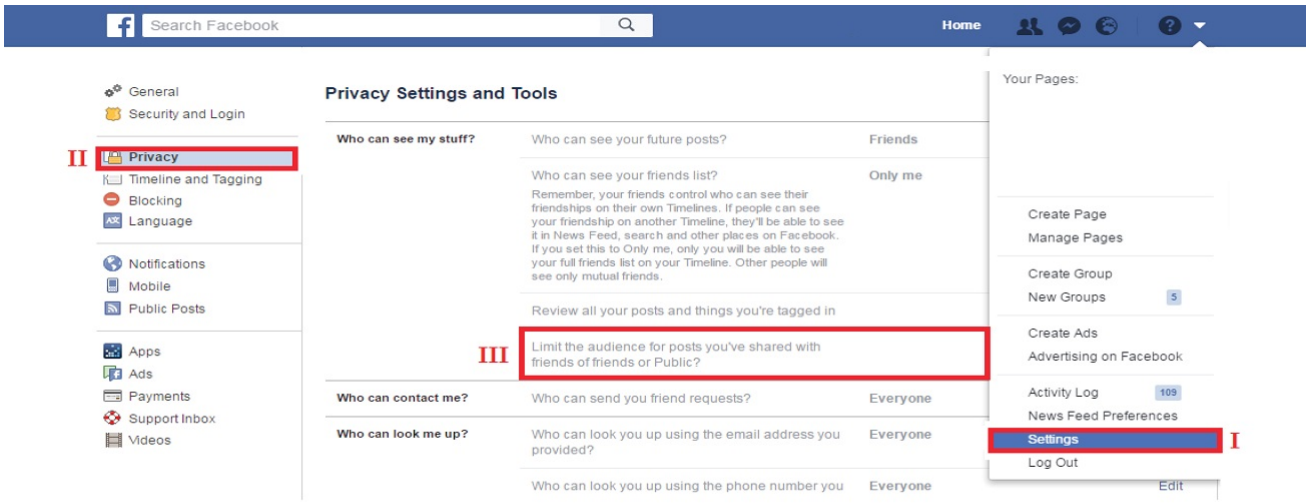


სურათი 13: „ჭკვიანი სიები“

ერთი მხრივ, სიები დაგეხმარებათ, მარტივად და სწრაფად განსაზღვროთ თქვენი პოსტის სამიზნე აუდიტორია, მეორე მხრივ, ის საშულებას გაძლევთ, ცალკე დაათვალიეროთ თითოეულ სიაში მყოფი მეგობრების მიერ გაზიარებული პოსტები.

ყველა ძველი პოსტის მხოლოდ მეგობრებისთვის გაზიარება

რაც შეეხება ძველ პოსტებს, რომლებიც ბევრია და შესაბამისად, რთულია გადამოწმება, საჯაროდ გაქვთ თუ არა გაზიარებული თითოეული მათგანი, Facebook გთავაზობთ ყველა ძველ პოსტზე აუდიტორიის წვდომის შეზღუდვის ფუნქციას. ამ გზით, თქვენი ძველი პოსტების ნახვას მხოლოდ მეგობრები შეძლებენ.

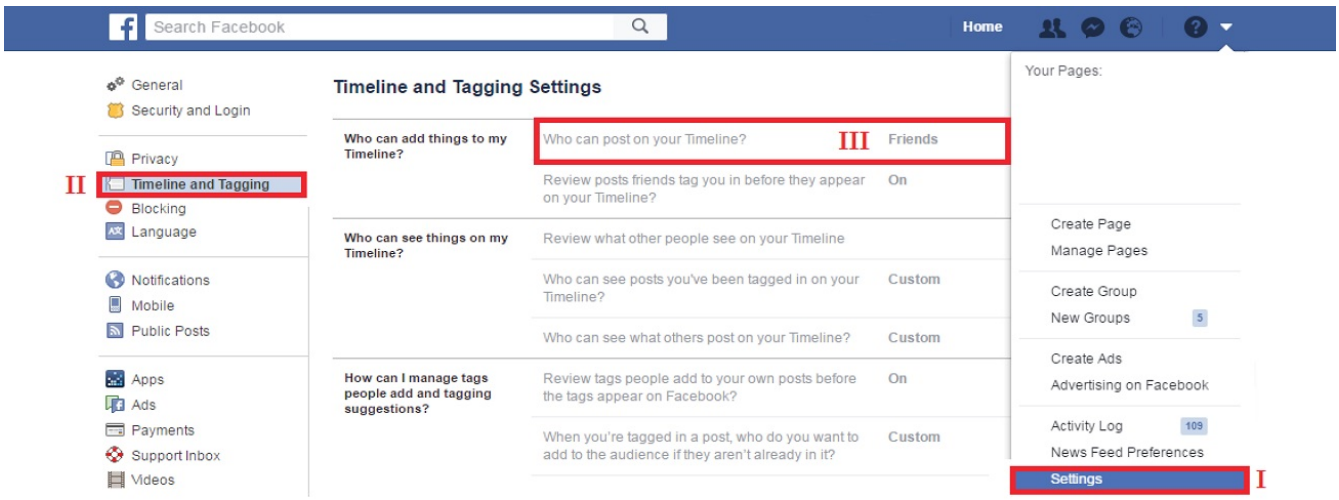


სურათი 14: როგორ გავააქტიურო ძველი პოსტების შეზღუდვა: I - აირჩიეთ პარამეტრები. II - ვის შეუძლია ნახოს ჩემი მასალები. III - შეზღუდეთ აუდიტორია.

მონიშვნის (tag) ფუნქცია

მონიშვნის უფლება

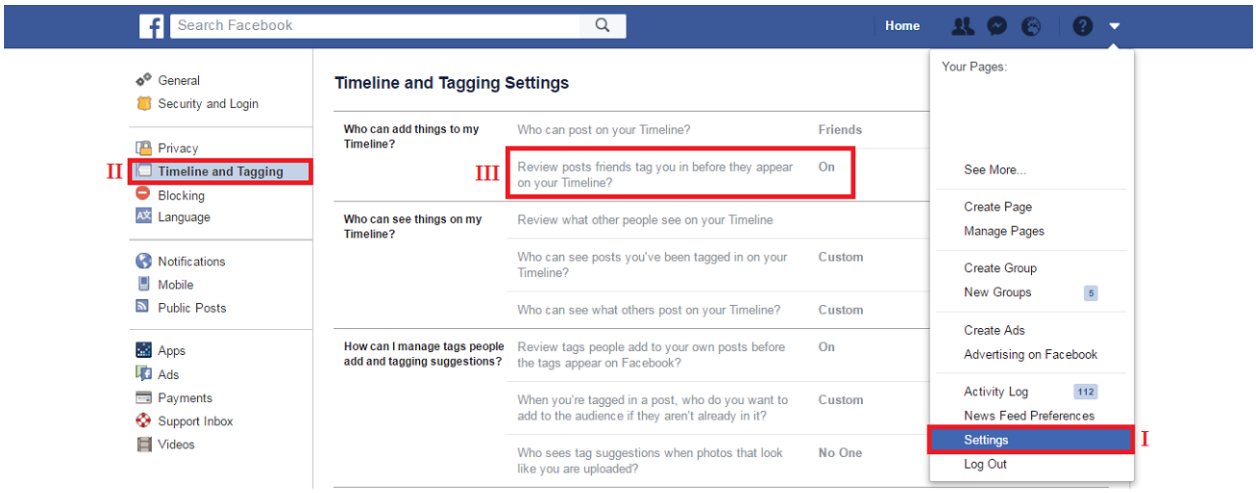
გააკონტროლეთ, თუ ვის აქვს თქვენს პირად გვერდზე თქვენივე პირადი ინფორმაციის გაზიარებისა და თქვენი ამა თუ იმ ფოტოზე მონიშვნის უფლება. ამ ფუნქციის გასააქტიურებლად გადადით პარამეტრების განყოფილებაში, აირჩიეთ ქრონოლოგია და მონიშვნა და თითოეულ ველში მონიშნეთ შესაბამისი აუდიტორია:



სურათი 15: <u>მონიშვნის უფლება</u>: I - აირჩიეთ პარამეტრები. II - ქრონოლოგია და მონიშვნა. III - ვის შეუძლია ჩემს პირად გვერდზე ინფორმაციის დამატება.

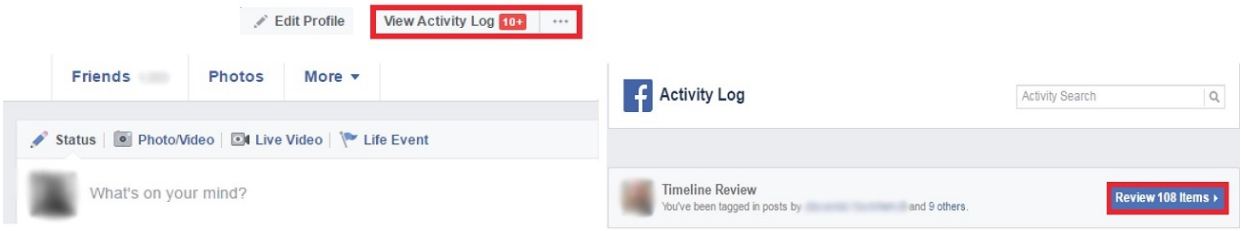
<u>თანხმობის მიცემა მონიშვნაზე</u>

ასევე შესაძლებელია, რომ თქვენი თანხმობის გარეშე ვერავინ შეძლოს თქვენი მონიშვნა.



სურათი 16: თანხმობა მონიშვნაზე: I - აირჩიეთ პარამეტრები. II - ქრონოლოგია და მონიშვნა. III - გადახედეთ მონიშნულ პოსტებს, სანამ გამოჩნდება თქვენს თაიმლაინზე. ამ ფუნქციის ჩართვის შემდეგ, ყოველ ჯერზე, როდესაც რაიმე აქტივობაზე მოგნიშნავენ, შეტყობინება მოგივათ.

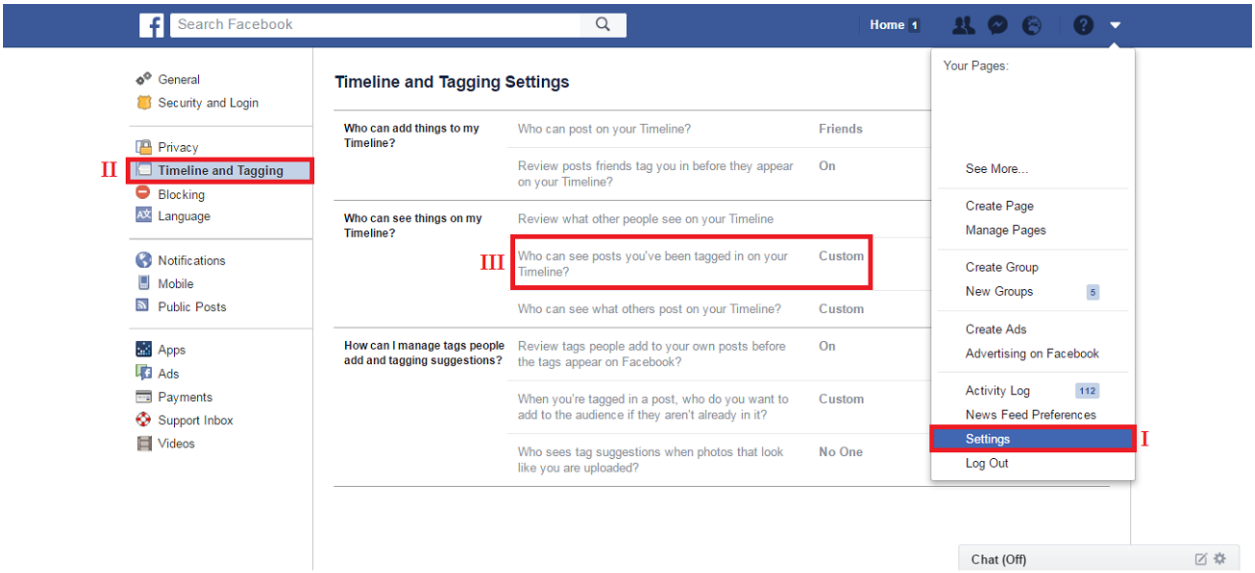
(პირადი გვერდიდან) გადადით აქტივობის პანელში→გადახედე მონიშნულ პოსტებს→ სურვილის შემთხვევაში კი დააჭერთ „თაიმლაინზე დამატება“-ს. თქვენი დასტურის გარეშე ინფორმაცია თქვენს გვერდზე არ გამოჩნდება!



სურათი 17: ფოტოების დამატების ინსტრუქცია

ვის შეუძლია ნახოს, რაზე ვარ მონიშნული

ცალკე შეგიძლიათ, შეზღუდოთ აუდიტორია, რომლისთვისაც ხელმისაწვდომი იქნება მასალა, სადაც თქვენ ხართ მონიშნული. შედეგად, შეგიძლიათ ეს მასალა თქვენი მეგობრების მხოლოდ კონკრეტულ ნაწილს გაუზიაროთ. სურვილის შემთხვევაში, ასევე შესაძლებელია, რომ ეს პოსტები მხოლოდ თქვენთვის ჩანდეს.

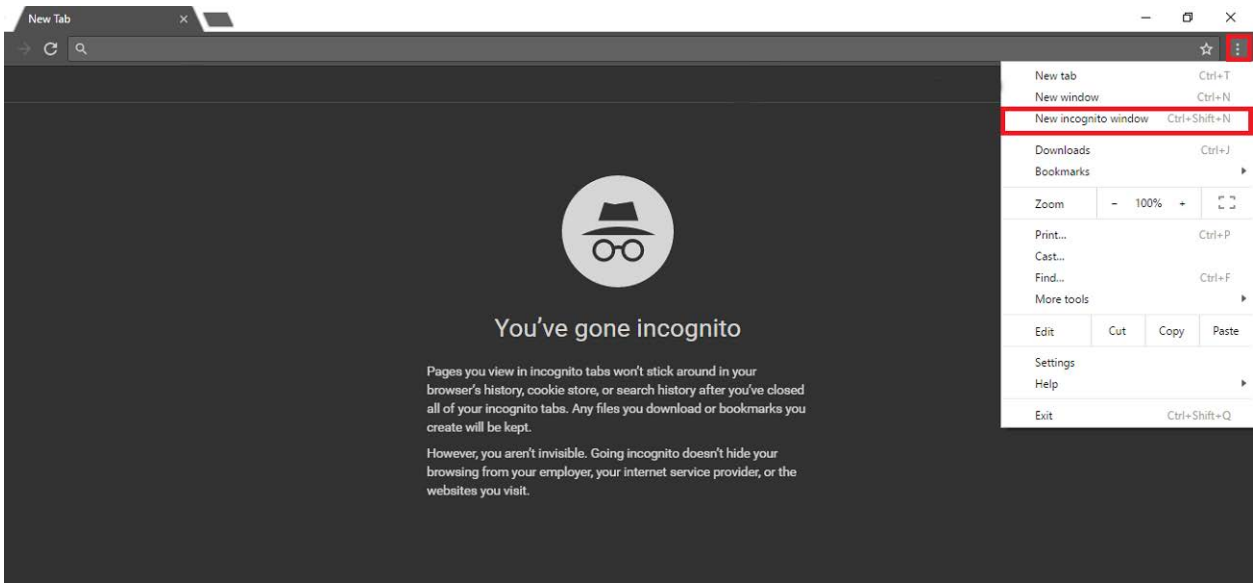


სურათი 18: მონიშნულ კონტენტზე წვდომის შეზღუდვა: I - აირჩიეთ პარამეტრები. II ქრონოლოგია და მონიშვნა. III- "Custom".

პირადი მონაცემების მართვა

ონლაინ რეკლამების თავიდან აცილება

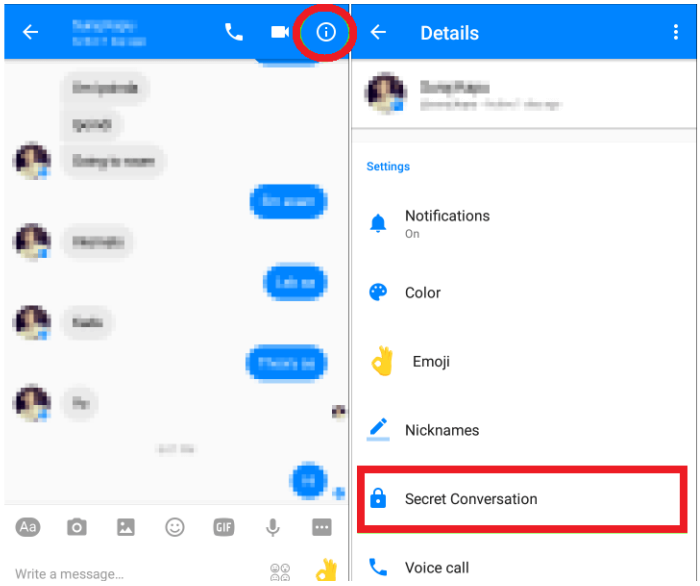
Facebook ძირითად შემოსავალს რეკლამებიდან იღებს და რეკლამის სამიზნე აუდიტორიების უკეთ შესარჩევად, იგი მომხმარებელთა ონლაინ აქტიურობის დაკვირვების უფლებას იტოვებს. თუ არ გსურთ, რომ Facebook-მა შეინახოს ინფორმაცია იმ ვებგვერდების შესახებ, რომლებსაც სტუმრობთ, მაშინ გამოიყენეთ „ინკოგნიტო ფანჯარა“ (Incognito Window), რაც ყველა ბრაუზერს აქვს, და რომელიც არ ინახავს ისტორიას და მისი დახურვის შემდეგ შლის თქვენს მაიდენტიფიცირებელ მონაცემებს.



სურათი 19: *ინკოგნიტო ფანჯრის გასახსნელად, გამოიყენეთ თქვენი ბრაუზერის მარჯვენა ზედა კუთხეში არსებული მენიუ ისე, როგორც ფოტოზეა ნაჩვენები.*

<u>პირადი მიმოწერის უსაფრთხოება</u>

Facebook-ის საშუალებით უაღრესად კონფიდენციალური ინფორმაციის გაზიარებისას შეგიძლიათ, გამოიყენოთ „საიდუმლო მიმოწერა". ასეთი ტიპის მიმოწერა მთლიანად დაშიფრულია და მისი წაკითხვა მიმღების მხარეს მხოლოდ იმ მოწყობილობაზეა შესაძლებელი, რომელზეც მიწერეთ.

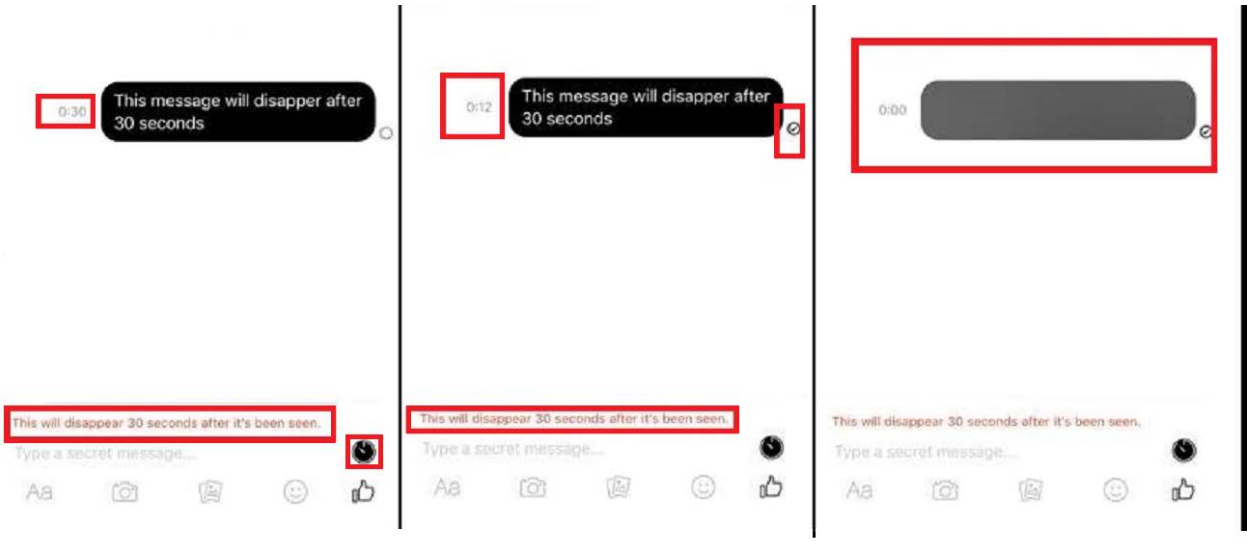


სურათი 20: *საიდუმლო მიმოწერა: გახსენით მესენჯერის მიმოწერის ფანჯარა და ზედა მარჯვენა კუთხეში არსებული ღილაკის საშუალებით გააქტიურეთ დაშიფრული მიმოწერა ისე, როგორც ფოტოზეა ნაჩვენები.*

რით განსხვავდება დაშიფრული მიმოწერა ჩვეულებრივი მიმოწერისგან?

დაშიფრული მიმოწერა ჩვეულებრივი მიმოწერის ანალოგიურად გამოიყენება, თუმცა არსებობს მცირედი განსხვავები:

- დაშიფრული მიმოწერისას ვერ გაგზავნით მოძრავ სურათებს (ე.წ გიფებს) და ვიდეოს;
- ვერ განახორციელებთ ხმოვან ზარს;
- დაშიფრული შეტყობინების გაგზავნის შემდეგ ადრესატი უნდა დაგთანხმდეთ მიმოწერის დაწყებაზე;
- შეგიძლიათ, დააყენოთ გარკვეული დრო, რომლის გასვლის შემდეგაც თქვენი შეტყობინება ავტომატურად წაიშლება.



სურათი 21: გახსენით მესენჯერის მიმოწერის ფანჯარა და ქვედა მარჯვენა კუთხეში არსებული ღილაკის საშუალებით დააყენეთ დრო, რომლის გასვლის შემდეგაც თქვენი შეტყობინება წაიშლება.

Facebook Messenger-იდან გამოსვლა სმარტფონებზე

სმარტფონებზე თქვენ დაინსატლირებული გაქვთ, როგორც Facebook-ის ისე მესენჯერის აპლიკაციები, თუმცა Facebook-იდან გამოსვლით მესენჯერი ჩართული რჩება. შესაბამისად, თუ ვინმე თქვენს ტელეფონს აიღებს, მას მთელი თქვენი მიმოწერის ნახვა შეეძლება.

Facebook Messenger-იდან გამოსვლის ინსტრუქცია IOS-ის მაგალითზე:[1]

1. გახსენით **Facebook** აპლიკაცია;

2. **Facebook**-ის მარჯვენა ქვედა კუთხეში არსებული მენიუს საშუალებით აირჩიეთ პარამეტრები;

[1] ინსტრუქცია შეგიძლიათ ნახოთ შემდეგ ვიდეოში: https://youtu.be/Qrs7_BH4cS8

3. აირჩიეთ "**Account Settings**", შემდეგ კი - "**Security**";

4. აირჩიეთ "**Facebook Messenger**" და ეკრანზე "**x**" სიმბოლოზე დაჭერით გათიშეთ აპლიკაცია.

Facebook Messenger-იდან გამოსვლის ინსტრუქცია Android-ის მაგალითზე:[2]

1. გადადით თქვენი სმარტფონის პარამეტრების განყოფილებაში;

2. აირჩიეთ "**Apps**";

3. აირჩიეთ **Messenger** აპლიკაცია;

4. Android 6.0 ვერსიის შემთხვევაში ეკრანზე გამოჩნდება "**Storage**";

5. მონიშნეთ იგი და აირჩიეთ "**Clear Data**", შემდეგ კი - "**Ok**".

[2] ინსტრუქცია შეგიძლიათ ნახოთ შემდეგ ვიდეოში: https://youtu.be/QIfbvn9E9Sg