



ციფრული უსაფრთხოება

თბილისი
2025

კიბერ და ციფრული უსაფრთხოება



ციფრული უსაფრთხოება არის
ციფრული მონაცემების დაცვა.

კიბერუსაფრთხოება გულისხმობს
მონაცემთა შენახვისთვის და ამ
მონაცემების მიმოცვლისთვის არსებული
ინფრასტრუქტურის დაცვისთვის
მიმართულ მუდმივ ძალისხმევას.



უსაფრთხოების ცნება

უსაფრთხოება არის მდგომარეობა, როდესაც დაზღვეული ხარ რისკებისგან და ზარალისგან/ზიანისგან, რომლებიც თავის მხრივ წარმოადგენენ ძალადობის ან სხვა წინასწარგანზრახული ქმედების შედეგს.



დაცვა არის მიღებული ზომების და ღონისძიებების ერთობლიობა, რომლებსაც იყენებენ უსაფრთხოების ხარისხის გასაზრდელად.

რისკების ფორმულა :

$$\text{რისკი} = \frac{\text{საფრთხეები} * \text{მონყვლადობები}}{\text{რესურსები}}$$

ცნებების განმარტება:

რისკი – რაიმე ზიანის მომტანი მოვლენის მომავალში მოხდენის ალბათობა

საფრთხე – ცოტა ხნის წინანდელი ან ჯერ კიდევ მიმდინარე მოვლენა, რომელიც აშკარად გამოხატავს, რომ არის ვნების/ზიანის/ზარალის მომტანი, ან ტოვებს ასეთ შთაბეჭდილებას

მოწყვლადობები – ნებისმიერი ფაქტორი, რომელიც ხელს უწყობს შესაძლებლობას მოგვაცენონ/მოგვადგეს ვნება და, ასევე, უწყობს ხელს მოგვადგეს უფრო მეტი ზარალი.

რესურსები – ნებისმიერი ფაქტორი, მოვლენა, ნივთი და ა.შ (უნარებისა და კონტაქტების ჩათვლით), რაც ხელს უწყობს უსაფრთხოების ხარაისხის გაზრდას.

https://www.frontlinedefenders.org/sites/default/files/flds_workbook.pdf

საფრთხეებისა და რისკების განსაზღვრის მაგალითი:

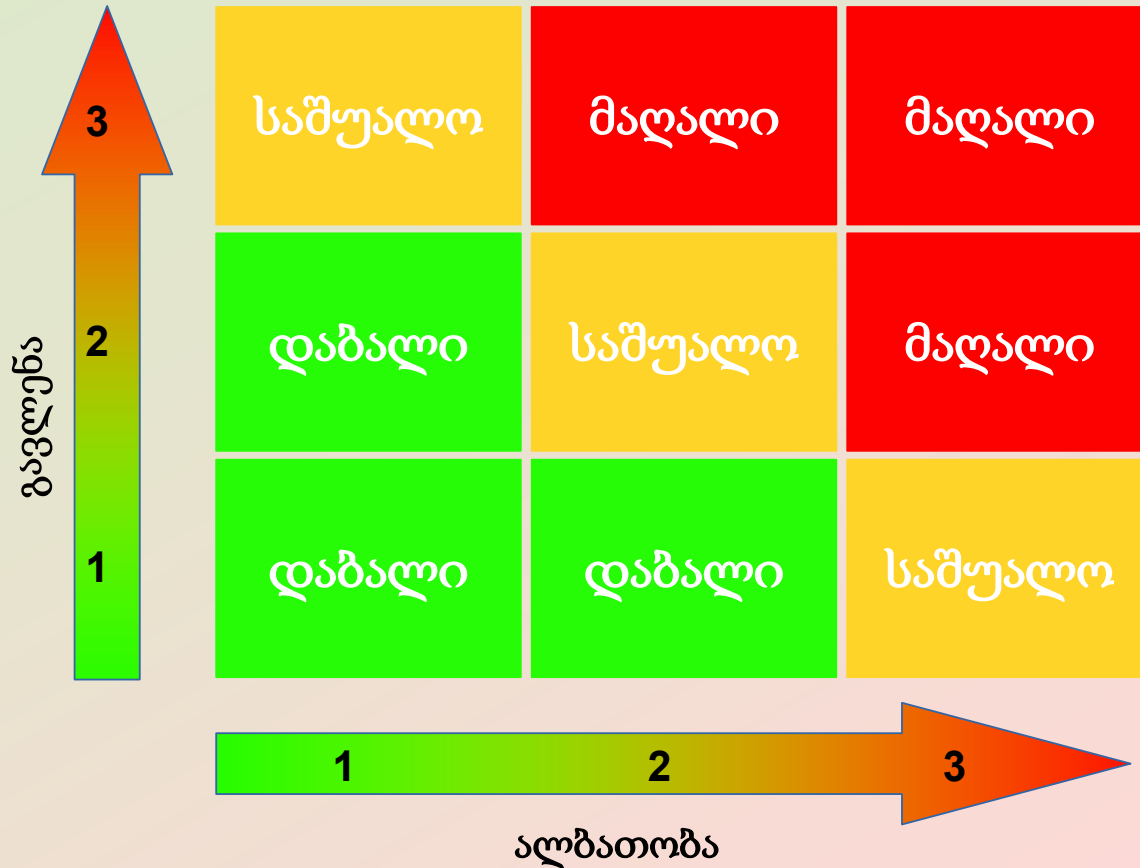
საფრთხე:

- ქვეყანაში კრიმინალის მაღალი დონეა

რისკი:

- მაღალია ალბათობა რომ მომპარავენ კომპუტერს
- . . .

რისკების რუკა (“შუქნიშანი”)



გავლენა:

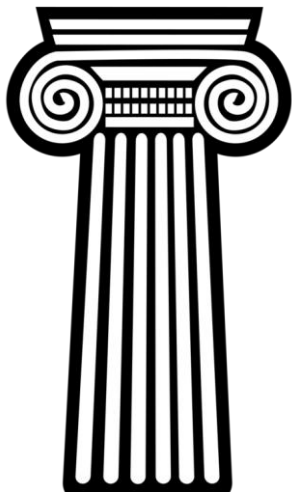
1. დაბალი
2. საშუალო
3. მაღალი

აღბათობა:

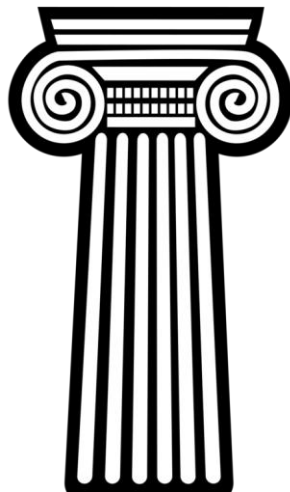
1. დაბალი
2. საშუალო
3. მაღალი

სამი დიდი ცრურწმენა

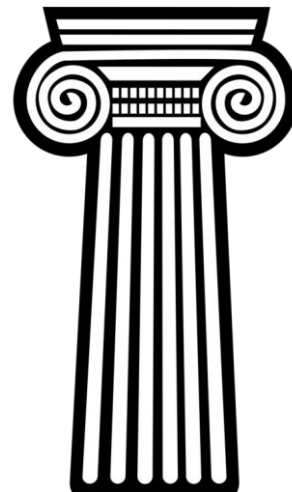
სავარაუდო რისკები



არაფერი მაქვს
დაასამალი!



ყველა მითვალთვალეს და
მითვალთვალეზ
გამუდმებით!



არაფერს აქვს აზრი...
ყველა შემთხვევაში, მაინც
დამჰკავენ...

რას ვიცავთ? აქტივები!

ფიზიკური აქტივები:

- კომპუტერები, ლეპტოპები
- სმარტფონები, პლანშეტები
- ინფორმაციის გარე მატარებლები
- როუტერები/ქსელი
- ამობეჭდილი ინფორმაცია
- ადამიანები (თანამშრომლები და სხვა საკვანძო პირები)

ციფრული აქტივები:

- მონაცემები
 - საფოსტო ექაუნტები
 - მესენჯერები
 - ექაუნტები სხვადასხვა პლატფორმაზე
 - ონლაინ იდენტობა
 - უსაფრთხოების კამერები
 - ლოკალური ქსელები
- და ა.შ.

რა შეიძლება დაემართოს აქტივს?

ფიზიკური აქტივები:

- მოპარვა
- დაკარგვა
- წართმევა/კონფისკაცია
- ფიზიკური დაზიანება/ზემოქმედება
- ...

ციფრული აქტივები

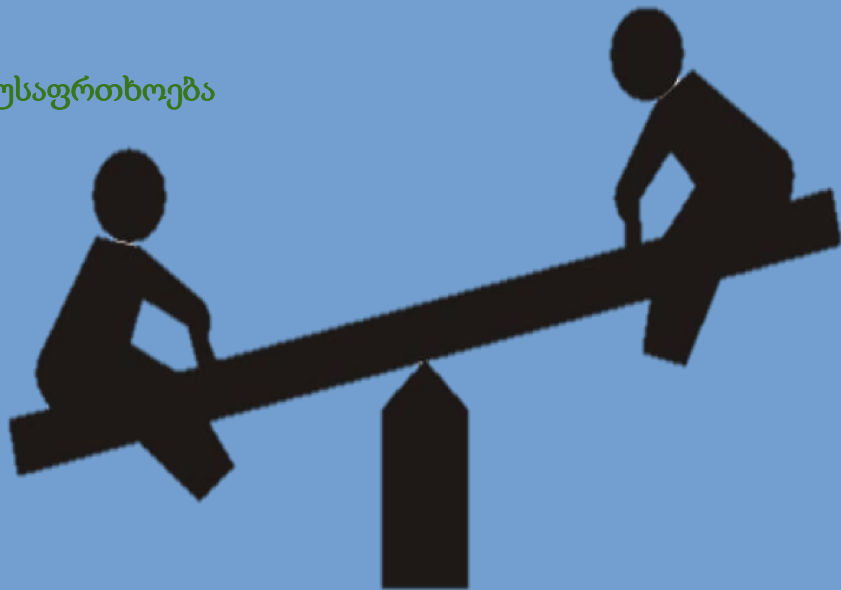
- გატეხვა/შელწევა
- არასანეცირებული წვდომა
- მონაცემებთან წვდომის დაკარგვა
- მონაცემების შეცვლა/ჩანაცვლება
- ონლაინ იდენტობის მოპარვა
- ...

!!!

მნიშვნელოვანია გვახსოვდეს, რომ ჩვენ ხელშია
არა მარტო ჩვენი არამედ ყველა იმ ადამიანის
უსაფრთხოება, რომელთა შესახებ ინფორმაცია
ინახება ჩვენს მოწყობილობებში და, რომ ჩვენს
შესახებ ინფორმაციაც ინახება სხვების
მოწყობილობებში.

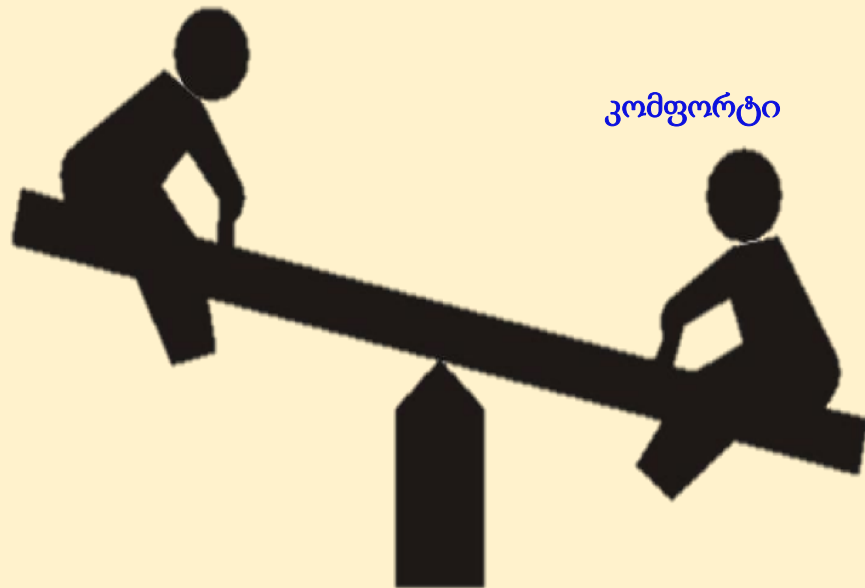
კომფორტი

უსაფრთხოება



უსაფრთხოება

კომფორტი



მოწყობილობების ფიზიკური უსაფრთხოება

- დაცული საოფისე სივრცე
 - ✓ მტკიცე კარი
 - ✓ ჟალუზები
 - ✓ სიგნალიზაცია/დაცვის სისტემები
- სეიფები/საცავები სარეზერვო ასლების შესანახად
- მოწყობილობებთან წვდომის მკაცრად განსაზღვრა

- მოწყობილობების შენახვა უსაფრთხო/დაცულ ადგილებში
- არ დატოვოთ მოწყობილობები უყურადღებოდ
- პორტატული მოწყობილობებისთვის საიმედო ბუდეები და შალითები
- თანამშრომლების და სხვა საკვანძო პირების დაცულობა
- ...

მონეტარიზაციის და მონაცემების დაცვა ფიზიკური უსაფრთხოება



მოწყობილობების ფიზიკური უსაფრთხოება

- დაცული საოფისე სივრცე
 - ✓ მტკიცე კარი
 - ✓ ჟალუზები
 - ✓ სიგნალიზაცია/დაცვის სისტემები
- სეიფები/საცავები სარეზერვო ასლების შესანახად
- მოწყობილობებთან წვდომის მკაცრად განსაზღვრა

- მოწყობილობების შენახვა უსაფრთხო/დაცულ ადგილებში
- არ დატოვოთ მოწყობილობები უყურადღებოდ
- პორტატული მოწყობილობებისთვის საიმედო ბუდეები და შალითები
- თანამშრომლების და სხვა საკვანძო პირების დაცულობა
- ...

კომპიუტერების ციფრული დაცვა

- ლიცენზირებული ოპერაციული სისტემები
- ლიცენზირებული პროგრამები
- ოპერაციული სისტემების და პროგრამების ჩამოტვირთვა სანდო წყაროებიდან
- შიფრირება
- კონფიდენციალურობის და უსაფრთხოების პარამეტრების კონფიგურაცია
- ანტივირუსების გამოყენება
- ფაიერვოლის გამოყენება
- ოპერაციული სისტემების და პროგრამების დროული და სისტემატიური განახლებები

სმარტფონების ციფრული დაცვა

- პასვორდი ან PIN-ი შესასვლელად (ეკრანზე)
- შიფრირება (მახსოვრობის ბარათებისთვის)
- PIN-კოდის გამოყენება SIM-ბარათისთვის
- SIM-ის მიბმა პასპორტთან (???)
- ლიცენზირებული პროგრამები საიმედო წყაროებიდან (F-Droid, Google Play, PLAYSTORE)
- ოპერაციული სისტემას უნდა ჰქონდეს აქტიური მხარდაჭერა
- კონფიდენციალურობის და უსაფრთხოების პარამეტრები
- პრივატულობის პარამეტრების შემოწმება
- ოპერაციული სისტემების და პროგრამების დროული და სისტემატიური განახლებები

დისკების შიფრირება

თანამედროვე ციფრული მოწყობილობები გვადლევენ საშუალებას დავშიფროთ მათი დისკები სადაც ინახება მონაცემები. ეს შესაძლებელია კომპიუტერებზე, სმარტფონებზე და მონაცემების გარე მატარებლებზეც.

მსგავსი დაცვა უზრუნველყოფს მონაცემების დაცვას არასანქცირებული წვდომისგან.

შიფრირება

- Windows → BitLocker, VeraCrypt
- MacOS → FileVault, VeraCrypt
- Android → მე-10 ვერსიიდან ნაგულისხმევად გააქტიურებულია. აუცილებელია ეკრანის დაბლოკვა.
- iOS → ნაგულისხმევად გააქტიურებულია. აუცილებელია ეკრანის დაბლოკვა
- Linux Distributions → LUKS, VeraCrypt

აქაუნტების დაცვა

- საიმედო პასვორდი



- ორფაქტორიანი აუთენტიფიკაცია

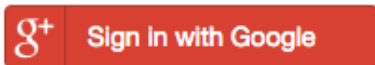
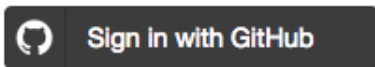
- Pop-up შეტყობინება
- CMC-კოდი
- OTP-კოდის პროგრამები
- USB-გასაღები
- სარეზერვო კოდები



ღია ავტორიზაცია (OAuth 2.0 → Open Authorization) ღირს თუ არა მისი გამოყენება???

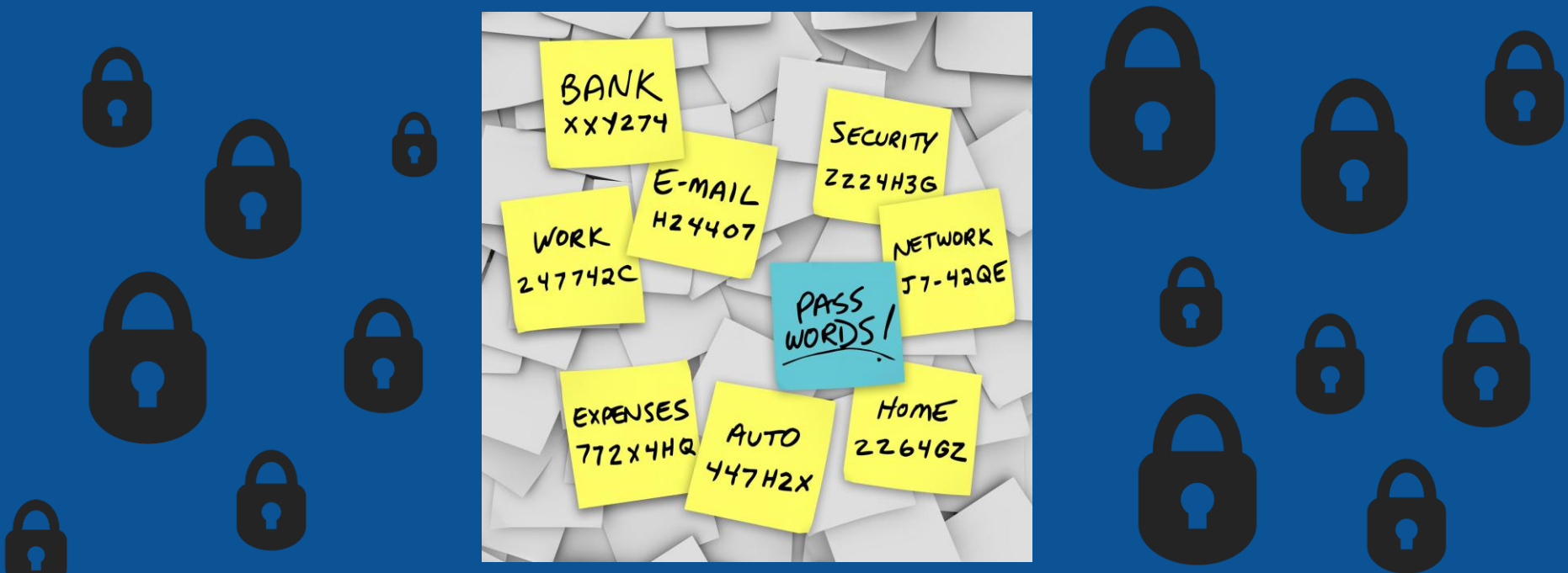
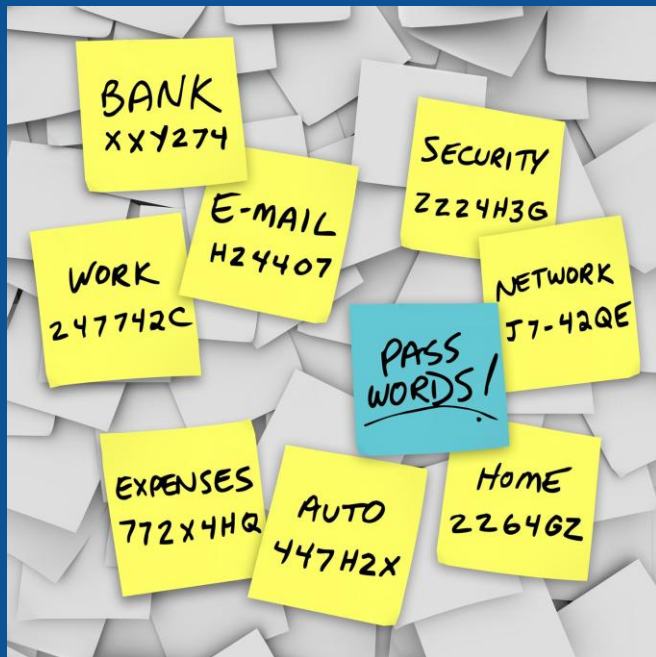
Sign In

Sign in using any of the following services:



პასვორდები და მათი გამოყენება

ყველა აქაუნთისთვის და მოწყობილობისთვის გამოიყენეთ ძლიერი და უნიკალური პასვორდები



როგორ შევქმნათ პასვორდები?

- არ გამოიყენოთ სიტყვები არცერთი ლექსიკონიდან ან ენციკლოპედიიდან;
- არ გამოიყენოთ გავრცელებული ორფოგრაფიული შეცდომები;
- არ გამოიყენოთ კომპიუტერის ან აქაუნტების სახლები
- გამოიყენეთ სულ ცოტა 12 სიმბოლო
- დიდი ასოები ((ABC...))
- პატარა ასოები (abc...)
- ციფრები (123...)
- სპეცსიმბოლოები (! @ # \$ % ^ & * ())



პასვორდების მაგალითები

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin\$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

ფრაზის მაგალითები

გამოდგება	Thisismypassphrase
კარგია	Acatthatlovesdogs
უკეთესია	AcatTh@tlov3sd0gs

ფრაზები როგორც პასვორდები

- შეარჩიეთ თქვენთვის ღირებული ფრაზა
- გამოიყენეთ სპეცსიმბოლოები:
! @ # \$ % ^ & * ()
- რაც უფრო გრძელია ფრაზა მით უკეთესია
- არ გამოიყენოთ ცნობილი ციტატები ან
ამონარიდები ცნობილი ნაწარმოებებიდან
- შეგიძლიათ შეადგინოთ და გამოიყენოთ
როგორც პასვორდი საკუთარი გრძელი
წინადადება



სად და როგორ შევინახოთ პასვორდები?

პასვორდების მენეჯერები



Rob Schultz / IDG



არსებობს პასვორდების შენახვის სხვა მაგალითებიც.
არცერთი მეთოდი არ ითვლება 100%-ით უსაფრთხოდ და უნიკალურად.

უსაფრთხო კომუნიკაცია



ელექტრონული ფოსტა

Gmail + Mailvelope



ProtonMail



Tutanota

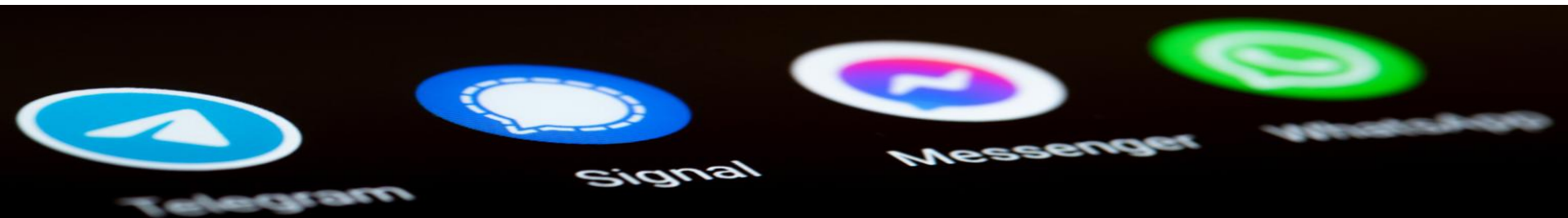


.

მესენჯერები

შერჩევის კრიტერიუმები:

1. E2E შიფრირება
2. ღია კოდი
3. რომელი ქვეყნის იურისდიქციაშია
4. რა მონაცემებს გასცემენ



გეოლოკაციის და იდენტიფიკაციის საფრთხე



1. ციფრული კვალის მინიმიზირება
2. TXIF-მონაცემების გასუფთავება
გასაჯაროების წინ
3. აქტივიზმისთვის სხვადასხვა „ნიკის“,
სხვადასხვა ფოსტის გამოყენება
4. გასაჯაროებული ინფორმაციის
მინიმიზირება
5. შესაძლებლისდაგვარად (კონტექსტიდან
გამომდინარე) გეოლოკაციის გათიშვა ან
გადაყვანა რეჟიმზე “მხოლოდ აპლიკაციის
გამოყენებისას”
6. თუ არ იყენებთ გათიშეთ Bluetooth და WiFi

კითხვები და პასუხები

