ოპერაციული უსაფრთხოება და პერსონალური მედეგობა: აღმოსავლეთ სამეზობლოს ქვეყნების მიმოხილვა

ოპერაციული უსაფრთხოება და პერსონალური მედეგობა: აღმოსავლეთ სამეზობლოს ქვეყნების მიმოხილვა

სახელმძღვანელო უცხო ქვყნის ავტორიტარული რეჟიმების მხრიდან კიბერ, ინფორმაციული, სადაზვერვო და პერსონალური უსაფრთხოების საფრთხეებზე და ქვეყნის შიგნით ხელწოლისა და შევიწროების საკითხებზე

ავტორები

საქართველო: მედიის განვითარების ფონდი – მარიამ პატარიძე, სოფო გელავა, თინათინ გოგოლაძე

მოლდოვა: IPIS - სტრატეგიული ინიციატივების ინსტიტუტი – ვიქტორია ოლარი

უკრაინა: უკრაინის კრიზისის მედია ცენტრი – ლიუბოვ ციბულსკა, ოლექსანდრა ცეხანოვსკა

ოპერაციული უსაფრთხოების რეკომენდაციები: უსაფრთხოების პოლიტიკის ევროპული ღირებულებების ცენტრის გუნდი

რედაქტორი

ანდრეა მიხალკოვა, უსაფრთხოების პოლიტიკის ევროპული ღირებულებების ცენტრი

ანგარიში მომზადდა ევროკომისიის ფინანსური მხარდაჭერით. წინამდებარე გამოცემაში წარმოდგენილი ფაქტები ან გამოთქმული მოსაზრებები არ უნდა იქნეს მიჩნეული ევროკომისიის პოზიციად. ევროკომისია არ იღებს პასუხისმგებლობას ანგარიშის შინაარსის ნებისმიერი სახით გამოყენებაზე. გამოქვეყნებული შინაარსი მთლიანად ავტორების პასუხისმგებლობაა.

ფოტოსურათზე საავტორო უფლება: გვ. 8: ხუან ანტონიო სეგალი / Flickr, გვ. 13: ვიაჩესლავ ბუნესკუ / Flickr

1. შესავალი

წინამდებარე ანგარიში სამოქალაქო საზოგადოების ორგანიზაციებსა (CSO) და ცენტრალური ევროპისა და აღმოსავლეთ სამეზობლოს ქვეყნების (EN) თინქ-თენქებს შორის ერთწლიანი თანამშრომლობის შედეგია. ეს არის ერთი ნაწილი პროექტისა მდგრადობასა და თავდაცვაში მიღებული გამოცდილების გაღრმავება და გაზიარება, რომელიც სამოქალაქო საზოგადოების შესაძლებლობებს აფასებს, თუ როგორ შეუძლიათ საქართველოში, უკრაინასა და მოლდოვაში ოპერაციული უსაფრთხოებისა და გავლენის მოხდენის უკანონო მეთოდების გამოვლენის შესახებ უსაფრთხოების პოლიტიკის ევროპული ღირებულებების ცენტრის (EVC) გზამკვლევის გამოყენება. ჩვენ მათი მიდგომების ადაპტირებას ვახდენთ და აღმოსავლეთ სამეზობლოს ქვეყნების პოლიტიკურ რეალობას ვარგებთ.

ავტორებმა შესაბამისი ღია წყაროებიდან ინფორმაციის მოპოვების, საზოგადოებრივი აზრის კვლევისა და საგამომძიებო ანგარიშების საშუალებით საფუძვლიანი სამაგიდე კვლევა ჩაატარეს. სამაგიდე კვლევა შესაბამის ექსპერტებთან და ადგილობრივ თანამდებობის პირებთან სტრუქტურირებული ინტერვიუების მეშვეობით განხორციელდა. ანგარიშში მოცემული ინფორმაციის უმეტესი ნაწილი მოგვაწოდეს, როგორც მედიის წარმომადგენლებმა, ასევე სამოქალაქო საზოგადოების ორგანიზაციებიდან საგარეო პოლიტიკისა და უსაფრთხოების ექსპერტებმა. თემის სენსიტიურობიდან გამომდინარე გადავწყვიტეთ, არ გამოგვექვეყნებინა რესპონდენტების სახელები, ამ ინფორმაციის მიღება უსაფრთხოების პოლიტიკის ევროპული ღირებულებების ცენტრის სარედაქციო გუნდისგან შეგიძლიათ .

ჩვენმა მკვლევრებმა ყურადღება გაამახვილეს მედიის მდგომარეობაზე საქართველოში, უკრაინასა და მოლდოვაში:

საქართველოში უცხოური მავნე გავლენის რამდენიმე შემთხვევის ანალიზი (case study) უკვე განხორციელდა, თუმცა, დეტალური და შედარებითი შეფასებებები უცხოური მავნე გავლენის სრული მასშტაბის შესახებ ნაკლებად არის გაკეთებული, შესაბამისად, კონკრეტული სტრატეგიული რეკომენდაციები სამოქალაქო საზოგადოების ადვოკატირების კამპანიებისათვის არ არის შემუშავებული. ევროკავშირისა და ნატოს ფარგლებს მიღმა მოქმედი რამდენიმე სახელმწიფო მავნე გავლენას ახდენს საქართველოში დიპლომატიური აქტივობების, ენერგეტიკული და ეკონომიკური პოლიტიკის ბერკეტების და საინფორმაციო ომის საშუალებით, ასევე, ქვეყნის შიგნით არსებულ იმ მარგინალური ან მეინსტრიმული ჯგუფების მხარდაჭერით, რომლებსაც სახელმწიფოსთვის ზიანის მიმყენებელი პოტენციალი გააჩნიათ. პოსტ-საბჭოთა ქვეყნები, როგორიც საქართველოა, განსაკუთრებით მოწყვლადები არიან აღნიშნული ჯგუფების მიერ გამოწვეული ზიანის მიმართ, რაც არა მხოლოდ კარგად არის დოკუმენტირებული აშშ-ისა და ევროკავშირის ანგარიშებში, არამედ საზოგადოებისთვისაც შესამჩნევია; ე.წ. „ბორდერიზაციის პროცესმა“ საქართველოს მოქალაქეებს ელექტროენერგიის გათიშვების სერია მოუტანა. საქართველოში კონკრეტული არასამთავრობო ორგანიზაციების, მედია საშუალებების,

გავლენის აგენტებისა და პოლიტიკური ძალების მეშვეობით განხორციელებული მტრული ქმედებები ქვეყნის ევრო-ატლანტიკური ინტეგრაციის პროცესის დისკრედიტაციასა და დემოკრატიული განვითარების მიმართ სკეპტიციზმის გაღვივებას ისახავს მიზნად. ბოლო საპრეზიდენტო არჩევნებმა, რომელიც 2018 წლის 28 ოქტომბერს ჩატარდა, ცხადყო, თუ რამდენად მჭიდროდ იყო რამდენიმე კამპანია დაკავშირებული კორუფციასთან და დეზინფორმაციასთან, რაც სამოქალაქო საზოგადოების ორგანიზაციების საქმიანობას უშლის ხელს[1].

უკრაინაშიც, ასევე, ბევრი გამოწვევა აქვთ იმ აქტორებს, რომლებიც ხელისუფლების მხრიდან ანგარიშვალდებულებას ითხოვენ. „ღირსების რევოლუციის“ შემდეგ, სამოქალაქო საზოგადოების ორგანიზაციებმა საჯარო პოლიტიკის საკითხების შესახებ ღია და თავისუფალი საქმიანობის უფლება მოიპოვეს, თუმცა, ბოლო პერიოდში (განსაკუთრებით, 2018 წლის ბოლოს, საპრეზიდენტო და საპარლამენტო არჩევნებამდე ერთი წლით ადრე) ისინი სახელმწიფოს მხრიდან უფრო მეტ ზეწოლას განიცდიან. სამოქალაქო აქვივისტთა დისკრედიტაციის მიზნით მთავრობამ შეიმუშავა ახალი კანონი, რომელიც კორუფციის წინააღმდეგ მომუშავე პირებისგან საკუთარი შემოსავლის და ქონების გასაჯაროებას მოითხოვდა[2]. საზღვარგარეთიდან ძლიერი კრიტიკისა და თავად აქტივისტების მასობრივი წინააღმდეგობის შედეგად ეს წინადადება უარყოფილი იქნა. სამოქალაქო საზოგადოების რამდენიმე ორგანიზაციასა და სამოქალაქო აქტივისტსისთვის პირდაპირი ფიზიკური და სიტყვიერი შეურაცხყოფაც მიუყენებიათ. უკრაინის აღმოსავლეთის რეგიონები განსაკუთრებით რთული არეალია, სადაც კორუმპირებული, პრორუსული ადგილობრივი ხელისუფლება და პოლიცია ჟურნალისტებზე განხორციელებული ფიზიკურ თავდასხმების მიმართ გულგრილობას იჩენს. ამის ყველაზე ნათელი მაგალითი კორუფციის წინააღმდეგ მებრძოლი ხერსონელი აქტივისტის, კატერინა ჰანძიუკის ისტორიაა, რომელსაც გოგირდის მჟავის გამოყენებით დაესხნენ თავს. ჰანძიუკი პოლიციასა და უსაფრთხოების ორგანოებს აკრიტიკებდა და შინაგან საქმეთა სამინისტროს რეგიონულ განყოფილებაში კორუფციას გმობდა. მან კორუფციის რამდენიმე შემთხვევაში პოლიციის ჩართულობის შესახებ ინფორმაცია გამოაქვეყნა. 3 თვის შემდეგ ის თავდასხმისას მიყენებული ჭრილობებისგან გარდაიცვალა.

სამოქალაქო საზოგადოების აქტორების პოზიციები მოლდოვაშიც შესუსტდა[3], კერძოდ, 2016 წლიდან, მას შემდეგ, რაც მთავრობა შეიცვალა და ძალაუფლება მოლდოვის დემოკრატიული პარტიის სრული კონტროლის ქვეშ არის. 2017 წელს იუსტიციის სამინისტრო ეცადა მიეღო კანონი, რომელიც უცხოური დაფინანსების მიმღები სამოქალაქო საზოგადოების

1 Crosby, Alan. “Sex, Lies, And Audiotape: Just Another Election Campaign In Georgia.” *RadioFreeEurope/RadioLiberty*. Accessed on October 24,2018. https://www.rferl.org/a/sex-lies-and-audiotape-presidential-election-campaign/29561804.html

2 “Ukrainian Civil Society Unites to Counter Mounting Threats.“ *Freedom House*. Accessed on April 18, 2018. https://freedomhouse.org/article/ukrainian-civil-society-unites-counter-mounting-threats

3 Macrinici, Sorina.”Shrinking space for Civil Society in Moldova.“ *The Soros Foundation Moldova*. Accessed on April, 2018. https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf

ორგანიზაციებს პოლიტიკურ აქტივობებსა და საკანონმდებლო ინიციატივებს აუკრძალავდა[4] ეს სადავო დებულებები 2018 წლის მარტის ბოლოს კანონპროექტში შეიტანეს, თუმცა მოგვიანებით ეს პროექტი ჩააგდეს. საარჩევნო სისტემაში სადავო ცვლილებების შეტანის წინააღმდეგ გამოსვლის შემდეგ, მოლდოვის სამოქალაქო საზოგადოების ორგანიზაციებს მუდმივად თავს ესხმიან საჯარო პირები და მმართველ პარტიასთან დაკავშირებული სხვა აქტორები[5], მათ შორის, მასმედია, ბლოგერები და ინტერნეტ-ტროლები. მოლდოვის რამდენიმე არასამთავრობო ორგანიზაცია 2016-2018 წლებში განხორციელებული თავდასხმების შესახებ იტყობინებოდა, რომლებიც ცილისმწამებლურ ბრალდებებსაც მოიცავდა, თითქოს მათ 2014 წელს 1 მილიარდი ევროს საბანკო თაღლითობაში ან "ლანდრომატის" სკანდალში ჩართულ პირებთან ჰქონიათ კავშირი. ბოლო შემთხვევებს შორის აღსანიშნავია სპარლამენტო გამოძიება რამდენიმე მოლდოველი აქტივისტის, ჟურნალისტისა და ორი ცნობილი ოპოზიციური ფიგურის მიერ ევროპის პარლამენტში გამგზავრების[6] შესახებ, რომელიც პოლონური არასამთავრობო ორგანიზაცია „ღია დიალოგის ფონდის" მიერ იყო დაფინანსებული. პარლამენტარები ამტკიცებდნენ, რომ ფონდი რუსეთის მარიონეტი იყო და მოლდოვაში პოლიტიკური სიტუაციის დესტაბილიზაციას ისახავდა მიზნად. ზოგიერთი მათგანის აზრით, მოგზაურობის მონაწილეების წინააღმდეგ გამოძიება სახელმწიფოს ღალატის ბრალდებით უნდა დაწყებულიყო. ხშირად მსგავსი ტიპის თავდასხმით ოპერაციებს თან ახლავს ხსენებული აქტივისტების პირადი მიმოწერების ან საუბრების გასაჯაროება სხვადასხვა შეტყობინების აპლიკაციის მეშვეობით, რაც აჩვენებს იმას, რომ მთავრობის ხმამაღალი კრიტიკოსები კიბერშეტევების მიმართ მოწყვლადები არიან.

სამოქალაქო საზოგადოების ორგანიზაციების ზოგადი მდგომარეობა აღნიშნულ სამ ქვეყანაში კრიტიკული იყო. ძალიან ცოტა რამ კეთდება მათ მხარდასაჭერად. აქედან გამომდინარე, ევროპული ღირებულებების ცენტრმა (EVC) ამ ქვეყნებში არსებული მდგომარეობის შესახებ ცნობიერების ამაღლება და ოპერაციული და უსაფრთხოების ექსპერტთან კონსულტაციების საფუძველზე შემუშავებული პირადი უსაფრთხოების საუკეთესო პრაქტიკის გაზიარება დაისახა მიზნად.

მიმდინარე სამუშაოებისათვის ძირითადი ხელისშემშლელი ფაქტორები საფრთხეების კატეგორიზაციის საფუძველზე განვსაზღვრეთ და შემდეგი რეკომენდაციები მოვამზადეთ.

4 RFE/RL's Moldovan Service. "Moldovan NGOs Reject Proposed Ban On Foreign Funding" *RadioFreeEurope/RadioLiberty*. Accessed on July 12, 2017. https://www.rferl.org/a/moldova-ngos-reject-foreign-funding-ban/28612337.html

5 Macrinici, Sorina."Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accessed on April, 2018. https://www.soros.md/files/publications/documents/Civil%20Society%20Macrinici.pdf

6 Dulgher, Maria."An outline of the 'Open Dialog' scandal. PAS and DTPP in the gunsight of the Moldovan Parliament." *Moldova.org*. Accessed on November 13, 2018. https://www.moldova.org/en/outline-open-dialog-scandal-pas-dtpp-gunsight-moldovan-parliament/

2. მეთოდოლოგია:საფრთხეების კატეგორიზაცია და მათზე რეაგირების რეკომენდაციები

კატეგორია	საფრთხე	რა უნდა გააკეთოთ	აღწერა	ზეპირი ან წერილობითი მუქარა მაგალითი
1	ზოგადი დაუმისამართებელი, სიძულვილის ენის ან მუქარის ნიშნის შემცველი წერილი	მიწერეთ მეილი საკონტაქტო პირს თქვენს ორგანიზაციაში[7] იმავე დღეს[8].	დაუმისამართებელი შეტყობინება, რომელიც უხეშად და ნეგატიურად აფასებს ორგანიზაციას, მუქარის ან ირიბი მუქარის დაკონკრეტების გარეშე.	"წამოწოლილხარ, ღმერთმა იცის ვინ გაფინანსებს. საკუთარი ხელებით მუშაობა ისწავლე. შენნაირი ებრაელები და პ***რასტები ცუდად დაამთავრებენ. ჩვენ მოგხედავთ."
2	დამისამართებული შეტყობინება მუქარის ნიშნით	იმავე დღეს მიწერეთ მეილი თქვენი ორგანიზაციის საკონტაქტო პირს, პირადად შეატყობინეთ თქვენს უფროსს/ თქვენი ორგანიზაციის უსაფრთხოების მენეჯერს.	დამისამართებული შეტყობინება მუქარის ნიშნით, გაგზავნილი უშუალოდ პირისთვის ან სამიზნე პირის მითითებით, მუქარის შემდგომი კონკრეტიზაციის გარეშე/ მუქარა არის მხოლოდ ირიბი; ანონიმური სატელეფონო ზარები აშკარა მუქარების გარეშე.	"როგორ ბედავ პრეზიდენტის ასეთ შეურაცხყოფას, პრიმიტიულო. მე შენ გაჩვენებ. მოუთმენლად ველი, თუ როდის ვნახავ შენი აშშ-ის მიერ დაფინანსებული ოფისების ცეცხლის ალში გახვევას. ვიცი სადაც ხართ, გონებაჩლუნგებო."
3	დამისამართებული მუქარის შემცველი შეტყობინება, ან უშუალო მუქარა	დაუყოვნებლივ დაურეკეთ თქვენს უფროსს/ თქვენი ორგანიზაციის უსაფრთხოების მენეჯერს.	კონკრეტული პირისადმი მიმართული შეტყობინება, რომელიც შეიცავს კონკრეტულ მუქარას ამ** პირის ან მისი საყვარელი ადამიანების მისამართით. შეიცავს არასაჯარო ინფორმაციას (მისამართი, სახელი) და უშუალო მუქარას.	"შენთვის გაფრთხილება არ იყო საკმარისი? როგორც ჩანს, მომიწევს სხვადასხვა "არგუმენტების" გამოყენება, ღორო. მოიცადე, ვიცი, სადაც ცხოვრობ – ნოვაკოვას 3."
4	ფიზიკური ინციდენტი	საჭიროების შემთხვევაში, დარეკეთ 911. დაუყოვნებლივ დაურეკეთ თქვენს უფროსს/ თქვენი ორგანიზაციის უსაფრთხოების მენეჯერს.	კონკრეტულ სამიზნე პირს ლეგიტიმური შეგრძნება აქვს, რომ მისდევენ, აშინებენ, ან ადგილი აქვს თავდასხმის მცდელობას ან პირდაპირ ფიზიკურ დაპირისპირებას.	შეგრძნება, რომ ვიღაცა მოგსდევს ქუჩაში. ნებისმიერი, თუნდაც არაპირდაპირი, დაშინების მცდელობა (უცნობი, რომელიც ამბობს, "შეწყვიტე, თორემ...", და შემდეგ მიდის).

7 კარგი იქნება, თუ ასეთი შემთხვევებისათვის ელ. ფოსტის სპეციალურ ფუნქციას გააქტიურებთ, რომელიც უსაფრთხოების მენეჯერს ავტომატიურად გადააგზავნის შეტყობინებებს.

8 წინასწარ ვემზადებით სცენარისთვის, როდესაც პირი შეიძლება უარესად მოიქცეს.

3. სამიზნე ქვეყნებში ყველაზე გავრცელებული საფრთხეების წყაროების სტრუქტურა

	მოლდოვა	საქართველო	უკრაინა
კიბერუსაფრთხოება	• DDoS შეტევა • ფიშინგი (ყალბი მეილებისა და ვებ-ბმულების მიღება)	• DDoS შეტევა • ფიშინგი (ყალბი მეილებისა და ვებ-ბმულების მიღება) • გამომძალველი ვირუსი (დაშიფრული მონაცემები) • მონაცემთა დაკარგვა (დოკუმენტები, კორესპონდენცია)	• DDoS შეტევა (ოპერაციების მოკლევადიანი და საშუალოვადიანი პარალიზება) • ფიშინგი • მონაცემთა დაკარგვა (დოკუმენტები)
ინფორმაციული უსაფრთხოება	• პაროლების გაჟონვა (Yahoo, Facebook) • ელ.ფოსტის გატეხვა (კომუნიკაციის გამჟღავნება), მონაცემების მოპარვა) • ონლაინ დისკრედიტაცია(ჭორები, ტყუილი, შეურაცხყოფა და ა.შ.) • ონლაინ იდენტობის მოპარვა (იმპერსონალიზაცია)	• პერსონალური მონაცემების გაჟონვა (მისამართი, ტელეფონის ნომერი და ა.შ.) • პაროლების გაჟონვა (Yahoo, Facebook) • ელ.ფოსტის გატეხვა (კომუნიკაციის გამჟღავნება, მონაცემების მოპარვა) • ონლაინ დისკრედიტაცია (ჭორები, ტყუილი, შეურაცხყოფა და ა.შ.) • ონლაინ იდენტობის მოპარვა (იმპერსონალიზაცია) • სმარტ ტექნიკის მეხსიერებაში შეღწევა და პირადი ინფორმაციის მოპარვა ამ მასალებით შანტაჟისათვის (განსაკუთრებით, მოზარდთა ფოტოები ან არასრულწლოვნების ფოტოები და ვიდეოები)	• ელ.ფოსტის გატეხვა (კორესპონდენციის გაჟონვა, მონაცემების მოპარვა) • ონლაინ დისკრედიტაცია (ინტერნეტბულინგი) • სოციალური მედიის და ექსპერტების ყალბი ანგარიშების შექმნა • დეზინფორმაციის კამპანიებისა და ოპერაციების შეტევები • შევიწროება და დისკრედიტაცია უცხოელი სუბიექტების მიერ (რომლებიც ხშირად რუსული მავნე ოპერაციების სამიზნეები ხდებიან) • შევიწროება ადგილობრივი თვითმმართველობის მხრიდან (ორგანიზაციის პოლიტიკური სარგებლისთვის; შევიწროება მმართველი პოლიტიკური პარტიის მხრიდან)
ძირითადი კონტრდაზვერვითი უსაფრთხოება	• საეჭვო აქტივობა ახლო მიდამოში (ჯაშუშობა, ცნობისმოყვარეობა, და ა.შ.) • მტრული ქვეყნის სადაზვერვო სამსახურის მიერ გადაბირების მცდელობა (პირდაპირი შეთავაზებები, წახალისება და ა.შ.) • მოწვევა (ყალბი) ინტერვიუსთვის • მოსმენა/თვალთვალი ტელეკომპანიაში დამონტაჟებული სპეციალური მოწყობილობის მეშვეობით		
პირადი (ფიზიკური) უსაფრთხოება	• დაშინება (მუქარა, დევნა) • შანტაჟი • ვანდალიზმი	• დაშინება (მუქარა, შეურაცხყოფა) • შანტაჟი • უმნიშვნელო დაზიანებები	• ბულინგი საერთაშორისო მოგზაურობების დროს (დაკავება რუსეთში, ბელარუსში, მოლდოვასა და სომხეთში) • ვანდალიზმი (ოფისის დარბევა)

უკრაინა

4. უკრაინა

კონტექსტი

უკრაინაში მოქმედ 10 არასამთავრობო ორგანიზაციას ოთხი თვის განმავლობაში ვთხოვდით დახმარებას გამოკითხვის ჩასატარებლად კიბერუსაფრთხოების მიმდინარე გამოწვევების, შესაძლო საფრთხეებისა და მათთან დაპირისპირებისა და დაძლევისთვის საჭირო ინსტიტუციური შესაძლებლობების შესახებ. წარმატებული მესამე სექტორის ფონზე რესპონდენტთა შედარებით მცირე რაოდენობა და ბევრი არასამთავრობო ორგანიზაციის წარმომადგენლის ან/და აქტივისტის მხრიდან გამოკითხვაში მონაწილეობის ნების არქონა თავისთავად რაღაცის მაჩვენებელია. ჩვენ ვვარაუდობთ, რომ მათმა მნიშვნელოვანმა ნაწილმა გამოკითხვაში მონაწილეობის მიღებაზე უარი სწორედ გამოკითხვის ჩატარების ერთ-ერთი მიზეზის გამო თქვა – აწუხებთ მათი პერსონალური მონაცემების დაცულობის საკითხი და ისიც თუ რამდენად რამდენად პატიოსნად მოეპყრობიან ამ ინფორმაციას. თუ აღნიშნული ჰიპოთეზა გამართლდა, ცნობიერების მეტად ამაღლება და შემდეგ კი ნდობის მოპოვება არის საჭირო საველე სამუშაოებისას, კვლევის მიზნის შესახებ რესპონდენტების ინფორმირების დროს, განსაკუთრებით კი მაშინ, როცა კიბერუსაფრთხოების „უცნობ წყლებში ყვინთავ“. გარდა ამისა, რესპონდენტებმა უნდა აჩვენონ, რომ გაცნობიერებული აქვთ და იციან ზემოაღნიშნულ უსაფრთხოების გამოწვევები და უნდა ჰქონდეთ ნდობა არა მხოლოდ პარტნიორების მიმართ, რომელსაც მიაწოდებენ ინფორმაციას, არამედ მათი უსაფრთხოების შესაძლებლობების მიმართაც, რადგან ჰაკერული შეტევებისა და სენსიტიური ინფორმაციის გაჟონვის ისეთი შემთხვევებია ცნობილი, როდესაც არა მხოლოდ სამიზნე დაზარალდა, არამედ ისიც, ვინც მასთან მჭიდრო კონტაქტში იყო.

10 გამოკითხული ორგანიზაციიდან ყველას მსგავსი გამოცდილება ჰქონდა: მათ, ვინც არასამთავრობო სექტორში დიდწილად დეზინფორმაციისა და პროპაგანდის წინააღმდეგ მუშაობს, ან შედარებით ნაკლებად, ადამიანის უფლებების დაცვაზე ფოკუსით. მხოლოდ ის ფაქტი, რომ აღნიშნული ორგანიზაციები კიბერ და ინფორმაციულ საფრთხეებს კარგად აცნობიერებენ, არ გვაძლევს საფუძველს ვივარაუდოთ, რომ უკრაინის მთელმა მესამე სექტორმა იცის, როგორ მართოს აღნიშნული საფრთხეები, მაშინ როდესაც მათ შესაძლოა საფრთხეების ამოსაცნობად იგივე უნარი არ ჰქონდეთ. აღნიშნულის გათვალისწინებით მონაცემები შემდეგ ტენდენციებს ავლენს:

ტრენინგი ოპერაციულ უსაფრთხოებაში

რესპონდენტთა უმრავლესობამ აღნიშნა, რომ უსაფრთხოების ტრენინგზე წვდომა არ ჰქონიათ ან ის მათთვის საკმარისი არ იყო. თუ ვინმემ მიიღო რაიმე ტიპის საგანმანათლებლო დახმარება ამ საკითხზე, ხშირად ეს პროტოკოლების ან/და

ინსტრუქციების სახით ხდებოდა, რაც არ არის იმდენად ეფექტიანი, როგორც ვორქშოპის ფორმატში პრაქტიკული სწავლება, მაშინაც კი, როდესაც ინფორმაცია კარგად გააზრებული და სრულად გამოყენებულია. ერთ-ერთმა კვლევაში ჩართულმა ორგანიზაციამ აღნიშნა, რომ ოპერაციულ უსაფრთხოებაში მსგავს ტრენინგებს ჩვეულებრივ თვითონ ატარებდა, თუმცა საკუთარი მედეგობის გაუმჯობესებასაც ისურვებდა. ეს ორი დონეზე არსებულ პრობლემას ასახავს, როდესაც შესაბამისი ინფორმაციის რამდენიმე მიმწოდებლიდან რომელიმეს, შესაძლოა, საფრთხეებთან გასამკლავებლად საუკეთესო და უახლეს ინსტრუმენტებზე არ აქვს წვდომა, თავის მწირ გამოცდილებას სხვებს უზიარებს, და ამავე დროს, თავად მოწყვლადი რჩება.

ოპერაციული უსაფრთხოების გზამკვლევის არსებობა

გამოკითხულთა შორის, სტანდარტული ოპერაციული უსაფრთხოების პროტოკოლი მხოლოდ ორ რესპონდენტს ჰქონდა. ერთი რესპონდენტი მესამე მხარის მიერ შემოთავაზებული გზამკვლევის პრაქტიკაში გამოყენებას ცდილობს, მაგრამ მაშინაც კი, როდესაც ის სწორად არის გამოყენებული, მითითებების შესასრულებლად პრაქტიკული უნარების არქონის გამო, ის ორგანიზაციის უსაფრთხოებას მაინც რისკის ქვეშ ტოვებს. სხვებს კონკრეტული მითითებები არ გააჩნიათ ან მათ ხელთ არსებულ რესურსებს მიმართავენ.

კრიზისის მართვა უსაფრთხოების ინციდენტების დროს

მხოლოდ ერთმა რესპონდენტმა განაცხადა, რომ თავისი ოფისის ინფორმაციული ტექნოლოგიების (IT) განყოფილებას მიმართავდა, რაც იმ ტექნიკური სპეციალისტების სიმცირეზე მეტყველებს, ვისაც შესაძლო კიბერთავდასხმებთან გამკლავება შეუძლია. უმრავლესობა აცხადებს, რომ კოლეგებს ან საერთაშორისო პარტნიორებს მიმართავდა. მცოდნე პარტნიორების გარეშე, აღნიშნული ორგანიზაციები ციფრული თავდასხმების მიმართ დაუცველები არიან. თუმცა, უცხოური დახმარება მწირია და ხშირად უკრაინის მედია-ლანდშაფტში არსებულ „შეიარაღებაზე“ არ არის მორგებული. საინტერესოა, რომ სამოქალაქო საზოგადოების ორგანიზაციების ნდობა სამართალდამცველების მიმართ იმდენად დაბალია, რომ ისინი როგორც დამხმარე საშუალება მხოლოდ ორმა რესპონდენტმა ახსენა. მიუხედავად პარტნიორებისა, გამოკითხვის ყველა მონაწილემ უსაფრთხოების დამატებითი ტრენინგების ჩატარების საჭიროებაზე გაამახვილა ყურადღება, ძირითადად მათ საქმიანობასთან დაკავშირებულ ინფორმაციასა და კიბერსფეროში, მაგარამ ასევე უსაფრთხოებასთან დაკავშირებული საკითხების გაძლიერების მიმართულებით. ისინი ასევე განიცდიან იმ შესაბამისი ადამიანური რესურსების (IT სპეციალისტები და ა.შ.) ნაკლებობას, რომელთაც უსაფრთხოებასთან დაკავშირებულ სხვადასხვა საკითხის შესახებ მიმართავდნენ.

უსაფრთხოების გამოწვევები

კიბერუსაფრთხოება

რესპონდენტთა უმრავლესობამ მონაცემთა გაჟონვის, პერსონალური ინფორმაციის დაკარგვის, DDoS შეტევის, ფიშინგის, და კიბერშეტევების სხვა ტიპის რისკის გამო შეშფოთება გამოხატა. მონაცემთა შენახვასა და დაცვას არსებითი მნიშვნელობა აქვს, იმის გათვალისწინებით, რომ ზოგიერთ ორგანიზაციას პირდაპირი ან ირიბი ბულინგი აქვს გამოცდილი. ინტერნეტ-ომისათვის მცირე მზადყოფნისა და მათ ხელთ არსებული შეზღუდული ფინანსური რესურსების გათვალისწინებით, არ არის გასაკვირი, რომ არასამთავრობო ორგანიზაციებისთვის კიბერუსაფრთხოების გამოწვევები ყველაზე გავრცელებულ დაბრკოლებად რჩება.

ინფორმაციული უსაფრთხოება

მიზანმიმართული დისკრედიტაცია და რეპუტაციისთვის ზიანის მიყენება ამ სფეროში დიდ გამოწვევას წარმოადგენს. პერსონალურ მონაცემთა უსაფრთხოებას და მათ შესაძლო დაკარგვას კომუნიკაციის საშუალებებიდან გაჟონვის გზით ასევე უდიდესი მნიშვნელობა აქვს.

პირადი უსაფრთხოება

რამდენიმე ორგანიზაცია შეშფოთებულია იმის გამო, რომ მათი წევრები შეიძლება დააპატიმრონ იმ ქვეყნებში (ბელარუსის მსგავსად, სადაც უკრაინიდან რამდენიმე არასამთავრობო ორგანიზაციის წარმომადგენელს ეს რეალურად გადახდათ თავს), რომლებსაც რუსეთის ფედერაციასთან მჭიდრო კავშირები აქვთ. ისინი ძალიან გარკვევით იხსენებენ კოლეგების მიმართ ბულინგის, პირდაპირი მუქარის (მათ შორის, ანონიმური), ქურდობის, თავდასხმისა და ქონების დაზიანების ფაქტებს, მიუხედავად იმისა, ბოლო ორი ინციდენტი აშკარად პოლიტიკურად მოტივირებული იყო თუ არა.

სამომავლო საფრთხეები

რესპონდენტების უმრავლესობა იმ საინფორმაციო საფრთხეებს პროგნოზირებს, რომლებიც მათი ორგანიზაციების დისკრედიტაციისკენ და რეპუტაციის დაზიანებისკენ არის მიმართული. მიუხედავად იმისა, რომ რუსეთის ფედერაციის მავნებლური და ძალადობრივი გავლენები კარგად არის ცნობილი თავდასხმების სამიზნე ქვეყნებში, ისინი მაინც შიშობენ, რომ საკუთარი სახელმწიფო იძიებს მათზე შურს იმ შემთხვევაში, თუ მათი პოზიტიურად წარმოჩენა არ მოხდება. მათ აქვთ ეჭვი, რომ ახლადარჩეული (2019 წელს) ადმინისტრაციული ორგანოები კომუნიკაციის ახალ პოლიტიკას შეიმუშავებენ, რომელიც არასამთავრობო ორგანიზაციების საქმიანობას მკაცრად შეზღუდავს, საიდუმლო უსაფრთხოების სამსახურებს ჩართავს ან ისეთ კიბერსაფრთხეებს გამოიყენებს, როგორიცაა პერსონალური მონაცემების გაჟონვა და ბულინგი.

საფრთხის წყაროები

როგორც ზემოთ აღვნიშნეთ, ზოგ რესპონდენტს აქვს შიში, რომ უკრაინის მთავრობა, და განსაკუთრებით, პრეზიდენტის პარტიის „ხალხის მსახური“ (Sluha Narodu) წარმომადგენლები, პრეზიდენტის წარმომადგენლები, და პრო-რუსული პოლიტიკოსები მათ საქმიანობას ხელს შეუშლიან. გარე, კერძოდ, რუსეთის ფედერაციისგან მომავალი საფრთხეები, კიდევ სხვა საზრუნავია, რომელიც რუსეთის მავნე ინფორმაციის შესახებ რესპოდენტების განსაკუთრებული ხარისხით სპეციალიზაციას ხსნის. ადგილობრივი კრიმინალური ჯგუფები, უფლებამოსილების ბოროტად გამომყენებელი საჯარო მოხელეების ჩათვლით, ხშირად ზეწოლას ახორციელებენ იმ სამოქალაქო საზოგადოების წარმომადგენლებზე, რომლებიც მსგავსი ფაქტების (ადგილობრივი კრიმინალური ჯგუფების არსებობის) გამოაშკარავებას ცდილობენ.


IVECO
UȘI MODERNE DE INTERIOR
Magazinul
"MARIȚA"
etajul 1
Centrul comercial
"DOMUS"
Pavilionul Nr. 114
62-75-16
63-75-17

მოლდოვა

5. მოლდოვა

სტრატეგიული ინიციატივების ინსტიტუტმა (IPIS) კიბერბულინგისა და კიბერუსაფრთხოების იმ გამოწვევების შესახებ ჩაატარა გამოკითხვა, რომლებსაც რუსეთის გავლენის, პროპაგანდის, დეზინფორმაციის, კორუფციისა და სხვა საკითხებზე მომუშავე ჟურნალისტები, არასამთავრობო ორგანიზაციები, აქტივისტები და მედიის წარმომადგენლები მოლდოვაში აწყდებიან. კითხვარის შესავსებად 10 რესპონდენტი შეირჩა. კითხვარების გაანალიზების საფუძველზე, შეიძლება შემდეგი პუნქტები გამოვყოთ:

ტრენინგი ოპერაციულ უსაფრთხოებაში

თითქმის ყველა რესპონდენტმა აღნიშნა, რომ ოპერაციულ უსაფრთხოებაში რომელიმე ეროვნული ან საერთაშორისო ორგანიზაციისგან დახმარება არ მიუღია. ზოგიერთმა ახსენა, რომ თვითნასწავლია, სხვა რესპონდენტებმა კი აღნიშნეს, რომ ამჯობინებენ ეს საკითხი მათი ორგანიზაციის ფარგლებს არ გასცდეს.

ოპერაციული უსაფრთხოების გზამკვლევის არსებობა

შეგვიძლია დავასკვნათ, რომ მოლდოვის რესპუბლიკის არასამთავრობო ორგანიზაციებს, აქტივისტებსა და მედიის წარმომადგენლებს შორის ოპერაციული უსაფრთხოების სახელმძღვანელოების, მითითებების ან პროცედურების გამოყენების პრაქტიკა ფართოდ გავრცელებული არ არის. თუმცა, მაინც შეგვიძლია რამდენიმე პოზიტიური ასპექტი აღვნიშნოთ. ორგანიზაციების უმრავლესობა ცდილობს თავი დაიცვას სტანდარტული ოპერაციული უსაფრთხოების გადაწყვეტების გამოყენებით, რომლებსაც Google-ი და Facebook-ი სთავაზობენ, კერძოდ, ორსაფეხურიანი ავტორიზაცია, ანტივირუსული პროგრამული უზრუნველყოფა, Firewall პროგრამები და ა.შ.

კრიზისის მართვა უსაფრთხოების ინციდენტების დროს

რესპონდენტთა უმრავლესობამ ახსენა, რომ უსაფრთხოების სფეროში კრიზისების დროს ისეთ სახელმწიფო ინსტიტუტებს, როგორებიცაა პოლიცია ან პროკურატურა, არ ენდობა და მათთან კონტაქტს მეტწილად ერიდება. ზოგიერთმა მათგანმა ისიც განაცხადა, რომ სახელმწიფო ინსტიტუტების მხრიდან მტრულ დამოკიდებულებას გრძნობს, ხოლო პოლიციისა და პროკურატურის მხრიდან ცინიკურ დამოკიდებულებას განიცდის. საინტერესოა, რომ ისეთ სიტუაციებში, როდესაც მათ თავს ესხმოდნენ, ავიწროებდნენ ან აშანტაჟებდნენ, ორგანიზაციებმა გადაწყვიტეს, რომ თავდაცვის საუკეთესო გზა ამგვარი ინციდენტების შესახებ საზოგადოების ინფორმირება იყო, რათა დარწმუნებულიყვნენ, რომ მსგავს შემთხვევებს მომავალში ადგილი აღარ ექნებოდა.

უსაფრთხოების გამოწვევები

კიბერუსაფრთხოება

რესპონდენტთა უმრავლესობამ სახელმწიფო აქტორების მხრიდან ტროლინგი და კიბერბულინგი უსაფრთხოების მთავარ გამოწვევად დაასახელა. ორგანიზაციები გამოძიებას ახორციელებენ და საზოგადოებას კორუფციის, ინტერესთა კონფლიქტებისა და მთავრობის წარმომადგენლების მიერ უფლებამოსილების ბოროტად გამოყენების ფაქტებს აცნობენ. რესპონდენტებმა ახსენეს, რომ მათ ვებგვერდებს თავს ესხმოდნენ, ხოლო ოფისებთან ახლოს საეჭვო მოწყობილობები აღმოაჩინეს.

ინფორმაციული უსაფრთხოება

თითქმის ყველა გამოკითხულს Facebook პაროლების გაჟონვის და ელექტრონული ფოსტის გატეხვის პრობლემა გამოუცდია. გარდა ამისა, ჟურნალისტების, სამოქალაქო საზოგადოების ორგანიზაციების აქტივისტების და ა. შ. მიზანმიმართული დისკრედიტაცია რესპონდენტების წუხილს იწვევს. ეს ხდება დუბლირებული ან ყალბი ანგარიშების შექმნით - ონლაინ იდენტობის მოპარვის გზით. აღნიშნული პრაქტიკა უფრო ინტენსიური გახდა 2019 წლის თებერვლის საპარლამენტო არჩევნების საარჩევნო კამპანიის დროს, როდესაც ბევრმა ჟურნალისტმა და სამოქალაქო აქტივისტმა აღმოაჩინა საკუთარი ორეული, რომელიც მისი სახელით სხვადასხვა საჯარო ჯგუფში კომენტარებს ტოვებდა. ამ შემთხვევაში, Facebook-მა მიიღო უპრეცედენტო გადაწყვეტილება და მოლდოვაში 168 Facebook ანგარიში, 28 გვერდი და რვა Instagram-ის ანგარიში გააუქმა (ზოგი მათგანი მთავრობის თანამდებობის პირებს ეკუთვნოდა), რადგან არსებობდა ეჭვი, რომ ისინი არჩევნების წინ ყალბ ამბებს, პოლიტიკურ პროპაგანდასა და არასწორ ინფორმაციას ავრცელებდნენ. Facebook -მა განაცხადა, რომ ამ საქმიანობაში ჩართული ადამიანები ცდილობდნენ დაემალათ საკუთარი იდენტობა, თუმცა საკითხის დეტალურმა შესწავლამ აჩვენა, რომ ამ აქტივობების ნაწილი მოლდოვის მთავრობის აპარატის თანამშრომლებს უკავშირდებოდა.

პირადი უსაფრთხოება

რამდენიმე რესპონდენტმა პროფესიული საქმიანობის შესრულების დროს თავდასხმების, მუქარის, ფიზიკური მეთოდებით დაშინების და მანქანის დაზიანების ფაქტების შესახებ გვამცნო. ზოგიერთი მათგანი უცნობი პირების, დანარჩენი კი სამართალდამცველი ორგანოების თანამშრომლების მიერ იყო განხორციელებული. მოძრაობის "Occupy Guguta" პროტესტის შემთხვევაში პოლიციამ აქტივისტებს ტერიტორიის გათავისუფლება აიძულა. ასევე, ბანერები და სხვა მასალებიც ჩამოართვა. უფრო მეტიც, მთავრობასთან დაკავშირებული სატელევიზიო არხები საპროტესტო მოძრაობის შესახებ ყალბი ამბების გავრცელებას ცდილობდნენ საეჭვო პირების, ალკოჰოლზე დამოკიდებული ადამიანების იმ ტერიტორიაზე შეგზავნით, სადაც საპროტესტო აქციას მიმდინარეობდა. აღნიშნულმა კი მომიტინგეების პირად უსაფრთხოებას პრობლემები შეუქმნა.

მომავალი საფრთხეები (შემდეგი 1-3 წლის განმავლობაში)

რესპონდენტთა უმრავლესობას შანტაჟი, დაშინება, სასამართალდევნა, შევიწროება და ფიზიკური თავდასხმა გამოცდილი აქვს. მათ ასევე ყურადღება გაამახვილეს კანონში შეტანილ ცვლილებებზე, რომელთაც მათ ყოველდღიურ საქმიანობაზე გავლენის მოხდენა შეუძლია, ესენია: კანონი სამოქალაქო ორგანიზაციების შესახებ, კანონი მედიის თავისუფლების შესახებ, კანონი უცხოური გრანტების შესახებ და კანონი ინფორმაციის ხელმისაწვდომობის შესახებ. თუ გავითვალისწინებთ საკითხებს, რომლებიც მათ ფოკუსს წარმოადგენს (ფინანსური დანაშაული, კორუფცია, უფლებამოსილების ბოროტად გამოყენება), პოტენციური საფრთხეები შესაძლოა შანტაჟი, შევიწროება ან ნათესავების უკანონო დაკავება იყოს. სხვა შესაძლო საფრთხეები შეიძლება შევიწროებას საგადასახადო ორგანოების მხრიდან ან თუნდაც საკანონმდებლო ორგანოს მხრიდან ეხებოდეს (საანგარიშო პერიოდში, პარლამენტს ჰქონდა ინიციატივა მოლდოვური არასამთავრობო ორგანიზაციების გარე დაფინანსება აეკრძალა).

საფრთხეების წყაროები

ყველა რესპონდენტმა აღნიშნა, რომ რისკის ძირითად წყაროს შიდა აქტორები წარმოადგენენ, კერძოდ, მთავრობა, რომელიც სამართალდამცავი ინსტიტუტების ან მოლდოვის მთავრობასთან დაკავშირებული პირების მეშვეობით მოქმედებს. თაღლითურ Facebook კამპანიებს რუსეთის ცნობილი „ტროლების ფერმის" ტაქტიკის გამოყენებით სწორედ ისინი ხელმძღვანელობდნენ. ეს ასევე გარედან ჩარევის შესაძლო საფრთხეს ქმნის, რადგან კრემლისტურმა აქტორებმა მსგავს სიტუაციებში სუსტი წერტილის გამოყენება კარგად იციან.


საქართველო

6. საქართველო

მედიის განვითარების ფონდმა (MDF) კიბერბულინგისა და კიბერუსაფრთხოების იმ გამოწვევებზე ჩაატარა კვლევა, რომელთაც რუსული პროპაგანდის, კორუფციისა და ადამიანის უფლებების საკითხებზე მომუშავე არასამთავრობო ორგანიზაციები, აქტივისტები და მედიის წარმომადგენლები აწყდებიან. შეირჩა 24 რესპონდენტი, რომელიც შერეული კითხვარის გამოყენებით გამოიკითხა. შეგროვებული მონაცემების ანალიზმა შემდეგი ტენდენციები გამოავლინა:

ტრენინგი ოპერაციულ უსაფრთხოებაში

რესპონდენტთა უმრავლესობისთვის ოპერაციულ უსაფრთხოებაში ტრენინგი ან სხვა პროცედურული ხასიათის დახმარება არ შეუთავაზებიათ. რამდენიმე რესპონდენტს მონაწილეობა ჰქონდა მიღებული ციფრულ უსაფრთხოებაზე ტრენინგში, რომაც ამ პირის/ორგანიზაციისთვის საჭირო საფრთხის თავიდან აცილების მექანიზმები სრულად არ მოიცვა.

ოპერაციული უსაფრთხოების გზამკვლევის არსებობა

რესპონდენტთა უმრავლესობა ოპერაციული უსაფრთხოების სახელმძღვანელოებს მათი ორგანიზაციული საქმიანობის განხორციელების დროს არ იყენებს. შიდა წესები მხოლოდ მცირე ნაწილს ჰქონდა შემუშავული .

კრიზისის მართვა უსაფრთხოების ინციდენტების დროს

რესპონდენტთა უმრავლესობამ აღნიშნა, რომ კიბერუსაფრთხოების ინციდენტების დროს მიმართავენ როგორც ორგანიზაციის IT სამსახურს, ასევე თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროსა და შინაგან საქმეთა სამინისტროს კიბერუსაფრთხოების განყოფილებას. როდესაც ისინი დანაშაულის ნიშნების შემცველ შემთხვევებს ავლენენ, პოლიციას ატყობინებენ.

ინფორმაციული უსაფრთხოების ინციდენტების შემთხვევაში (პერსონალური მონაცემების ხელყოფა), რესპონდენტები ამ ფაქტის შესახებ პერსონალურ მონაცემთა დაცვის ინსპექტორს და იშვიათ შემთხვევაში, სახალხო დამცველს ატყობინებენ.

ზოგ რესპონდენტს არ გააჩნდა ინფორმაცია იმის შესახებ, ვის შეიძლება მიმართოს სხვადასხვა ინციდენტების დროს პრობლემის მოსაგვარებლად და შესაბამისი ზომების მისაღებად.

თითქმის ყველა რესპონდენტს ციფრულ (პაროლი, შიდა ქსელების უსაფრთხოება, გამომძალველი ვირუსის ამოცნობა, როცა მონაცემები დაშიფრულია) და ინფორმაციულ (პერსონალური მონაცემების დაცვა) უსაფრთხოებაში ტრენინგის გავლა სჭირდება. რესპონდენტთა უმრავლესობამ აღნიშნა კრიზისების დროს პრობლემების ეფექტიანად მოგვარებისთვის

საჭირო უნარების განვითარების მნიშვნელობა. რამდენიმე რესპონდენტმა აღნიშნა, რომ კრიზისულ სიტუაციაში მოქმედების გეგმის შემუშავებაში დახმარება სჭირდებოდა.

უსაფრთხოების გამოწვევები

კიბერუსაფრთხოება

რესპონდენტთა უმრავლესობამ ულტრანაციონალისტური ჯგუფებისა და სამთავრობო აქტორების მხრიდან ტროლინგი და კიბერბულინგი უსაფრთხოების უმთავრეს გამოწვევად დაასახელა. განსაკუთრებით აღსანიშნავია ე.წ. სახელისუფლებო ტროლინგი, მთავრობის საქმიანობისადმი კრიტიკული მასალების გამოქვეყნების გამო.

მნიშვნელოვან გამოწვევებს შორის რესპონდენტებმა ასევე დაასახელეს ფიშინგი და ჰაკერული თაცდასხმები ორგანიზაციების ოფიციალურ ვებ-გვერდებზე ინფორმაციის მოპოვების მცდელობით. 2015 წელს MDF-ის მითების დეტექტორის ვებგვერდი (www.eurocommunicator.ge) ორჯერ გახდა ვინმე Luxas Hacker-ის მიერ განხორციელებული ჰაკერული თავდასხმის სამიზნე. პირველი თავდასხმის დროს, ჰაკერის გამოვლენა შეუძლებელი იყო, მაგრამ მეორე თავდასხმისას დადგინდა, რომ შეტევა განხორციელდა IP მისამართიდან, რომელიც თურქეთში იყო რეგისტრირებული. YouTube-ზე ატვირთულ ვიდეოებში ნათლად ჩანს "Dark Mirror" ვებსაიტის მისამართი http://dark-mirror.org. ვებგვერდზე თავდასხმების განხორციელებისას, ჰაკერი ბმულს იყენებდა.

2019 წლის 28 ოქტომბერს საქართველოზე მასშტაბური კიბერშეტევა განხორციელდა. ჰაკერების თავდასხმის შედეგად დაზიანდა საქართველოს მთავრობის და კერძო სააგენტოების, ასევე მედიასაშუალებებისა (TV პირველი, იმედი, მაესტრო, თრიალეთი და საქინფორმი) და არასამთავრობო ორგანიზაციების (მედიის განვითარების ფონდი) სერვერები.

დაჰაკული ვებსაიტების მთავარი გვერდები შეიცვალა. ვებგვერდების გახსნისას, საქართველოს ყოფილი პრეზიდენტის, მიხეილ სააკაშვილის ფოტო წარწერით "I'll Be Back"(„მე დავბრუნდები")ჩნდებოდა.

გატეხილი ვებგვერდები ადგილობრივი ვებ ჰოსტინგის მიმწოდებლის, კომპანია „პროსერვისის" სერვერებზე იყო განთავსებული. კომპანიის თანახმად, კიბერშეტევის შედეგად მწყობრიდან 15,000-მდე ვებ-გვერდი გამოვიდა. შინაგან საქმეთა სამინისტროს განცხადებით, გამოძიება საქართველოს სისხლის სამართლის კოდექსის 284 და 286 მუხლებით დაიწყო, რაც გულისხმობს კომპიუტერულ სისტემაში უნებართვო შეღწევას, ასევე კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის ხელყოფას.

საქართველოს საგარეო საქმეთა სამინისტროს 2020 წლის 20 თებერვლის განცხადებით, ქართული მხარის, გაერთიანებული სამეფოს გამოძიებისა და საერთაშორისო პარტნიორებთან თანამშრომლობის შედეგად მიღებული ინფორმაციის შესაბამისად, აღნიშნული კიბერშეტევა დაიგეგმა და განხორციელდა რუსეთის ფედერაციის შეიარაღებული ძალების გენერალური შტაბის მთავარი სამმართველოს (გრუ) მიერ.

ინფორმაციული უსაფრთხოება

რადიკალური ჯგუფებისა და სახელისუფლებო ტროლების მხრიდან რესპონდენტთა გამიზნული დისკრედიტაცია იმის უზრუნველსაყოფად, რომ მათ მიერ გავრცელებულმა ინფორმაციამ ლეგიტიმურობა დაკარგოს, გამოკითხულებმა ფართოდ გავრცელებულ პრობლემად დაასახელეს. რაც შეეხება ინფორმაციულ უსაფრთხოებას, რესპონდენტთა უმრავლესობამ პერსონალური მონაცემების (ანგარიშებში უნებართვოდ შეღწევა, ინფორმაციის გაჟონვა, კომუნიკაციის მონაცემების გასაჯაროვება, იდენტობის მოპარვა ინტერნეტში) გამჟღავნების საკითხი გამოჰყო.

პირადი უსაფრთხოება

რამდენიმე ორგანიზაცია გახდა თავდასხმის, მუქარისა (ფიზიკური ანგარიშსწორება, გაუპატიურება) და აგრესიის სამიზნე ულტრანაციონალისური ჯგუფების მხრიდან, რომლებიც ბოლო წლების განმავლობაში კიდევ უფრო გაძლიერდნენ. გამოკითხული ჟურნალისტები ფიზიკური და ქონებრივი დაზიანებების შემთხვევებზე (აპარატურისა და მანქანის დამტვრევა) საუბრობდნენ. რამდენიმე რესპონდენტი ფიზიკური თავდასხმის ობიექტი, ჟურნალისტური საქმიანობის შესრულებისასთან დაკავშირებული მოტივით გახდა.

ტელეკომპანია რუსთავი 2-ის ჟურნალისტი, დავით ერაძე ულტრანაციონალისტური მოძრაობა „ქართული მარშის“ წევრების ფიზიკური ანგარიშსწორების სამიზნე გახდა (2018); უფრო მეტიც, მის სახლს ესროლეს და ტყვიის მასრები სახლის აივანზე იქნა ნაპოვნი ჟურნალისტური საქმიანობისას მომზადებული სიუჟეტის გამო (2019);

„ტაბულას“ ჟურნალისტებს თავს დაესხნენ რესტორანში. თავდასხმელებმა მიზეზად „ტაბულას“ მიერ მათ მიერ ეკლესიის კრიტიკა დაასახელეს (2016).

გარდა ამისა, სხვადასხვა მედიასაშუალებების 39 წარმომადგენელმა ფიზიკური დაზიანებები მიიღო 21 ივნისის ანტისაოკუპაციო მიტინგის დარბევის დროს, პროფესიული მოვალეობების შესრულებისას.

მომავალი საფრთხეები (შემდეგი 1-3 წლის განმავლობაში)

რესპონტენტების უმრავლესობას სჯერა, რომ ტროლინგი და კიბერბულინგი ულტრანაციონალისტური ჯგუფების და სამთავრობო აქტორების მხრიდან, ასევე ონლაინ დისკრედიტაცია, პერსონალური მონაცემების გამჟღავნება და მუქარა შემდეგი 1-3 წლის განმავლობაშიც გაგძელდება. მათ თანახმად, ზოგიერთი ორგანიზაცია/წარმომადგენელი შეიძლება ფიზიკური თავდასხმებისა და დაპატიმრებების სამიზნე გახდეს.

საფრთხეების წყაროები

საფრთხეების მთავარ წყაროებს შორის რესპონდენტებმა დაასახელეს შიდა აქტორები – სახელმწიფო სტრუქტურები, მათ მიერ დაქირავებული და წახალისებული სიძულვილის ჯგუფები და მარგინალიზებული აქტორები, მათ შორის, ტროლები.

რაც შეეხება გარედან მომდინარე საფრთხეების მთავარ წყაროებს, რესპონდენტებმა კრემლისტური აქტორები და მათი სატელიტები (კერძო პირები და ორგანიზაციები) დაასახელეს, რადგანაც გამოკითხულთა ნაწილი რუსეთის გავლენებთან დაკავშირებულ საკითხებზე მუშაობს.

რესპონდენტებმა აღნიშნეს, რომ საერთაშორისო დონორებისგან/მთავრობებისგან დახმარება აღნიშნული საფრთხეებზე რეაგირებისათვის არ მიუღიათ.

7. რა შეიძლება გაკეთდეს? რეკომენდაციები არასამთავრობო ორგანიზაციებისა და სამოქალაქო აქტივისტთათვის

არასამთავრობო ორგანიზაციებმა უნდა იხელმძღვანელონ ძირითადი წესებით, რომელიც კიბერ, ინფორმაციულ, სადაზვერვო და პირადი უსაფრთხოების მიმართულებებს მოიცავს.

ინფორმაციის სენსიტიურობის დონეები

როგორც წესი, ინფორმაციული უსაფრთხოების სამ დონეს გამოყოფენ. კლასიფიკაციის ძირითადი კრიტერიუმი არის პოლიტიკური, პირადი და უსაფრთხოების დონის მნიშვნელობა ორგანიზაციებისთვის, ინდივიდებისთვისა და საზოგადოებისთვის.

კლასიფიკაციის მიზანი დროის მიერ კარგად გამოცდილი პრინციპის "გჭირდება იცოდე" უზრუნველყოფაა - სენსიტიური ინფორმაცია მხოლოდ მას მიეწოდება, ვისაც ის კონკრეტული მიზეზების გამო სჭირდება.

სენსიტიურობის დონე	მნიშვნელობის კრიტერიუმი	სად შეგვიძლია ინფორმაციის პერსონალურად განხილვა	სად შეიძლება ინფორმაციის ელექტრონულად განხილვა
0	მარტივი ოპერაციული ინფორმაცია, რომელიც არ არის პოლიტიკურად სენსიტიური ან არ მოითხოვს დაცვას, დე -ფაქტო საჯარო ინფორმაცია.	ნებისმიერ ადგილას	ყველგან: e-mail, Facebook და ა.შ.
1	**შიდა ინფორმაცია** (არასაჯარო პოლიტიკური ინფორმაცია, რომელიც არ წარმოადგენს საფრთხეს ეროვნული უსაფრთხოებისათვის, ან მასთან დაკავშირებული პირებისათვის)	მხოლოდ დანიშნულ შეხვედრაზე, ან პასუხისმგებელ პირთან ერთად, ელექტრონული მოწყობილობების გარეშე.	მხოლოდ Signal (შეტყობინება ან ზარი) ან ProtonMail, მაგრამ არა e-mail, ტექსტური შეტყობინება, ან სატელეფონო ზარი
2	**ძალიან სენსიტიური ინფორმაცია** (ეხება ეროვნულ უსაფრთხოებას, კონფიდენციალური წყაროების ვინაობას, პოლიტიკურად სენსაციური ინფორმაცია)	მხოლოდ დანიშნულ შეხვედრაზე, იმ პიროვნებასთან, ვისაც ეს ეხება, ელექტრონული მოწყობილობების გარეშე.	**არსად, მხოლოდ პირადად ელექტრონული მოწყობილობების გარეშე**

ორგანიზაციის თითოეულმა წევრმა უნდა მიიღოს და დაიცვას უსაფრთხოების ზომები ხუთი მიმართულებით:

- მოწყობილობებისა და პროფილების ძირითადი კიბერნეტიკული უსაფრთხოება
- სოციალური მედიის უსაფრთხოება
- კომუნიკაციების უსაფრთხოება
- მონაცემთა უსაფრთხოება
- პირადი უსაფრთხოება

მოწყობილობებისა და პროფილების ძირითადი კიბერნეტიკული უსაფრთხოება

a. უსაფრთხოების ძირითადი წესები

ვფიქრობთ, რომ თქვენ მხოლოდ ფართოდ გავრცელებულ ოპერაციულ სისტემებს იყენებთ. კლასიკური კომპიუტერების შემთხვევაში, ეს არის Windows-ი და macOS-ი, ხოლო პორტატული კომპიუტერების (i.e. ტაბლეტები და მობილური ტელეფონები) შემთხვევაში, iOS-ი და Android-ი. Apple-ის პროდუქტები (თუმცა მნიშვნელოვნად უფრო ძვირია) ყველაზე უსაფრთხო მოწყობილობებად მიიჩნევა, მას Android-ი მოსდევს. ჩვენ დაბეჯითებით გირჩევთ, რომ არ გამოიყენოთ Lenovo-ს რომელიმე პროდუქტი.

i. i. პაროლის დაყენება

წესი #1: ჩვენ ვიყენებთ სხვადასხვა პაროლებს სხვადასხვა ანგარიშებისთვის (სხვადასხვა ციფრები, სპეციალური სიმბოლოები და ა.შ.). Mozilla-ს ვებგვერდზე არის მოკლე სახელმძღვანელო იმაზე, თუ როგორ გავაკეთოთ ეს.

წესი #2: პაროლი უნდა შედგებოდეს მინიმუმ 22 სიმბოლოსგან და შეიცავდეს ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს.

წესი #3: იდეალურ შემთხვევაში, პაროლები უნდა შეიცვალოს სამ თვეში ერთხელ. მოსახერხებელია შეხსენების კალენდარის დაყენება.

წესი #4: პაროლებს მხოლოდ ქაღალდზე ვწერთ (რომელიც ინახება მხოლოდ ჩვენთვის ცნობილ ადგილას, და არა ჩვენს სამუშაო ადგილას. თითოეულ პაროლში ყოველთვის უნდა გამოტოვოთ მინიმუმ ერთი სიმბოლო, რათა ფურცლის დაკარგვის შემთხვევაში, ვერავინ გამოიყენოს) და არასოდეს კომპიუტერში შენახულ ტექსტურ დოკუმენტებში. არსებობს გამონაკლისი პაროლის მენეჯერების სახით, როგორებიცაა LastPass-ი ან KeePas2-ი. კიდევ ერთი ინსტრუმენტი პაროლების დაცულობისათვის შეიძლება იყოს ე.წ. ელექტრონული საკეტი (iOS – iCloud Keychain, Windows – Smart Lock, alt. 1Password), რომლის გამოყენებასაც გირჩევთ ორფაქტორიანი ავტორიზაციის ან დისკის დაშიფრვის დროს (იხილეთ ქვემოთ).

ii. ორფაქტორიანი ავტორიზაცია = პაროლთან ერთად უნდა შეიყვანოთ გენერირებული კოდი

წესი #5: ორფაქტორიანი ავტორიზაცია უნდა გააქტიუროთ ყველა იმ მოწყობილობაზე, რომელიც ამის საშუალებას იძლევა. კოდი ტექსტური შეტყობინებით ან მობილური აპლიკაციის მეშვეობით შეგიძლიათ მიიღოთ. ჩვენ გირჩევთ, რომ არ გამოიყენოთ ტექსტური შეტყობინებით ავტორიზაცია და დააყენოთ Google Authenticator-ი. სხვა თუ არაფერი, ეს მნიშვნელოვანია Facebook-ისთვის, Twitter-ისთვის, Google-ისთვისა და ინტერნეტ-ბანკინგისათვის. არ გირჩევთ სახის ამოცნობის ტექნოლოგიის გამოყენებას.

- ვებგვერდი სწრაფი რეაგირების კოდს (QR code) გიჩვენებთ, რომელიც შეგიძლიათ მობილური აპლიკაციის

გამოყენებით დაასკანეროთ. მას დაემატება კითხვის ნიშნის ქვეშ არსებული ანგარიში. ყოველ 30 წამში ერთხელ, აპლიკაცია გთავაზობთ ახალ უნიკალურ კოდს, რომელიც მისი მოქმედების ვადაში უნდა გამოიყენოთ. აპლიკაციის გამოსაყენებლად, თქვენ არ დაგჭირდებათ ინტერნეტ კავშირი ან მობილური ტელეფონის სიგნალი; თქვენი მოწყობილობა სინქრონიზებული იქნება სერვერთან მათი პირველად დაკავშირების შემდეგ. უნივერსალური ინსტრუმენტები: Google Authenticator (iOS, Android), Authy.

წესი #6: მუშაობის დასრულების შემდეგ, ყოველთვის გამოდით თქვენი მოწყობილობიდან, რათა თქვენს შემდეგ ნებისმიერ პირს ხელახლა შესვლა დასჭირდეს. ასევე გირჩევთ დამატებითი პაროლისა და თითის ანაბეჭდის გამოყენებას მნიშვნელოვან აპლიკაციებში შესასვლელად (Signal, Wickr Me, ProtonMail).

წესი #7: არასოდეს შეხვიდეთ თქვენს ძირითად პროფილებზე (Google, Facebook, ინტერნეტ-ბანკინგი) სხვა ადამიანის მოწყობილობების მეშვეობით, თუ განსაკუთრებული აუცილებლობა არ არის. შესვლის შემთხვევაში, შემდეგ შეცვალეთ პაროლები. Facebook-ის კონფიდენციალურობის პარამეტრებში ჩართეთ შეტყობინებები სხვა უცნობი მოწყობილობებიდან თქვენს ანგარიშზე შესვლის შესახებ, უმჯობესია ელექტრონული ფოსტის მეშვეობით. დააყენეთ firmware პაროლი თქვენი Mac-ის სერიის მოწყობილობაზე.

წესი #8: თუ თქვენ საეჭვო ელექტრონულ წერილს ან პირად შეტყობინებას მიიღებთ, გადაუგზავნეთ ის თქვენს თანამშრომლებს მკაცრი გაფრთხილებით (საგანში და შეტყობინების ძირითად ნაწილში) რომ არ გახსნან ის, არამედ გადააგზავნონ cert.incident@nukib.cz-ზე. საჭიროების შემთხვევაში, NUKIB-ის სპეციალისტები დაგეხმარებიან შემდგომი ნაბიჯების გადადგმაში (ე.ი. გამომძალველი ვირუსის შემთხვევაში და ა.შ.).

b. ანტივირუსი

წესი #9: ისეთ ოპერაციულ სისტემებს, როგორიცაა Windows 10, უკვე აქვთ ჩაშენებული ანტივირუსი (Windows 10). ზოგადად, არ არსებობს საჭიროება, რომ დააყენოთ მესამე მხარის მიერ შემოთავაზებული ფასიანი ანტივირუსული პროგრამა. თუ თქვენ იყენებთ ასეთ პროგრამას, თავი შეიკავეთ Kaspersky-ს ლაბორატორიის პროდუქტებისგან (არსებობს გონივრული ეჭვი, რომ ის დაკავშირებულია რუსულ სადაზვერვო სამსახურებთან), Huawei ან ZTE (რამდენადაც არსებობს გონივრული ეჭვი, რომ ისინი თანამშრომლობენ ჩინეთის სადაზვერვო სამსახურებთან). ჩვენ გირჩევთ Avast Antivirus-ს ან Eset-ს. დაბეჯითებით გირჩევთ, რომ არ გამოიყენოთ ჩინური ანტივირუსული პროგრამული უზრუნველყოფა (ე.ი. Qihoo 360, Tencent PC Manager). გირჩევთ, რომ ერთდროულად გამოიყენოთ 2 ანტივირუსული პროგრამა. გადმოწერეთ პროგრამა VirusScanner-ი.

წესი #10: კიბერთავდასხმების უმრავლესობა ხორციელდება ელექტრონული ფოსტის მეშვეობით – ფიშინგის გზით. ვირუსების წინააღმდეგ ფუნქციონალური დაცვის საფუძველი - არ გახსნათ უცნობი ადრესატებისგან მიღებულ მეილში მიმაგრებული დოკუმენტები. იყავით განსაკუთრებით ფრთხილად თუ მიმაგრებულ ფაილს აქვს

გაფართოება, როგორიცაა .exe, .pkg, .dmg ან .app. გარდა ამისა, არ დაგავიწყდეთ, რომ გადაამოწმოთ წერილის გამგზავნის ნამდვილობა, სანამ გახსნით მიმაგრებულ დოკუმენტს. გახსოვდეთ, რომ ფაილები .pdf ან .doc. ფორმატებშიც შეიძლება შეიცავდეს მავნე პროგრამას. მოთხოვნის შემთხვევაში, ყოველთვის უარი თქვით „მაკროსების ჩართვაზე" Excel-ში. თუ რომელიმე პირი ბმულს გიგზავნით, უმჯობესი იქნება, თუ დააკოპირებთ მას virustotal.com-ში, რადგანაც ის გარკვეულ წარმოდგენას შეგიქმნით იმაზე, თუ რამდენად სანდოა. გამოიყენეთ წესი #8.

თუ დარწმუნდით, რომ თქვენი კომპიუტერი მავნე პროგრამით დაინფიცირდა, ყველაზე უსაფრთხო და საუკეთესო გზა არის კომპიუტერული მედიის დისკის გასაწმენდი ინსტრუმენტით გაწმენდა. გადააყენეთ ოპერაციული სისტემა და აპლიკაციები და დააკოპირეთ თქვენი მონაცემები სარეზერვო ასლებიდან (მას შემდეგ, რაც გადაამოწმეთ, რომ სარეზერვო ფაილები არ არის დაინფიცირებული).

თუ გაქვთ ეჭვი, რომ მოწყობილობები დაინფიცირებულია, დაუყოვნებლივ გააკეთეთ სკანირება მავნე პროგრამულ უზრუნველყოფაზე (malware). მაშინაც კი, თუ სკანერი საფრთხეს არ აღმოაჩენს, იყავით პროაქტიული და დაიცავით მოცემული წესები. თუ მცირე ეჭვი მაინც გაქვთ, გამოიყენეთ მეორე ანტივირუსი.

აუცილებელი ნაბიჯები:

i. <u>WINDOWS</u>

ნაბიჯი 1: გამორთეთ კომპიუტერი ქსელიდან. გაუშვით მავნე პროგრამების საწინააღმდეგო (anti-malware) სკანერი (სასურველია სკანერის გაშვება განახლებული ანტივირუსის მქონე გარე მყარი დისკის მეშვეობით).

ნაბიჯი 2: გააქტიურეთ უსაფრთხო რეჟიმი. გასააქტიურებლად, გამორთეთ თქვენი კომპიუტერი და ხელახლა ჩართეთ. შემდეგ, როგორც კი ეკრანზე რამე გამოჩნდება, განმეორებით დააჭირეთ ღილაკს FS. როგორც წესი, უნდა გაიხსნას Advanced Boot Options მენიუ. აირჩიეთ ამ მენიუში უსაფრთხო რეჟიმი და დააჭირეთ ღილაკს Enter.

ნაბიჯი 3: წაშალეთ დროებითი ფაილები. როდესაც უსაფრთხო რეჟიმში ხართ, დროებითი ფაილები უნდა წაშალოთ დისკის გასუფთავების ინსტრუმენტის გამოყენებით. ამისთვის:

- გადადით გაშვების მენიუში (Start menu);
- ყველა პროგრამა ან უბრალოდ პროგრამები);
- Accessories-System Tools, Windows-ის ადმინისტრაციული ინსტრუმენტები (ვერსიიდან გამომდინარე)
- დისკის გასუფთავება;
- გადახედეთ ფაილებს წასაშლელი ობიექტების ჩამონათვალში და აირჩიეთ დროებითი ფაილები.

  აღნიშნული ფაილების წაშლით თქვენ ასევე ამოშლით მავნე პროგრამას, რომელიც დაიწყებდა მოქმედებას მაშინ, როდესაც თქვენი კომპიუტერი იტვირთებოდა

ნაბიჯი 4: ჩამოტვირთეთ და გაუშვით ვირუსების სკანერი. თუ თქვენი კომპიუტერი დაინფიცირდა, მაგრამ თქვენმა ანტივირუსულმა პროგრამამ არ გამოავლინა ვირუსი, ის უნდა ჩამოტვირთოთ (სხვა კომპიუტერზე), ხოლო შემდეგ გადაიტანოთ პირველ კომპიუტერში და დააყენოთ (ან გაუშვათ):

- „real-time" სკანერი, როგორიც არის AVG Antivirus free ან Avast Free Antivirus-ი, კომპიუტერს მავნე პროგრამებზე ფონურ რეჟიმში ასკანერებს, როდესაც იყენებთ თქვენს კომპიუტერს;
- მოთხოვნადი ოპერაციული სისტემის სკანერი, როგორიც არის Microsoft Safety Scanner-ი. თუმცა, ყოველთვის, როცა დასკანერებას აპირებთ, პროგრამა უნდა გაუშვათ მანუალურად.

  მავნე პროგრამის მოსაშორებლად, შესაძლოა ორივე ტიპის სკანერის გამოყენება დაგჭირდეთ. მავნე პროგრამების საწინააღმდეგო სკანერის ტიპიდან გამომდინარე, შეიძლება ინტერნეტთან ხელახლა დაკავშირება და დამატებითი პროდუქტის ჩამოტვირთვა დაგჭირდეთ.

  შესაძლოა დაგჭირდეთ ვირუსის მანუალურად მოშორება. ამის გაკეთება რეკომენდირებულია იმ შემთხვევაში, თუ Windows Registry-ის გამოყენების გამოცდილება გააჩნიათ და იცით, თუ როგორ გამოაჩინოთ და წაშალოთ სისტემური და პროგრამული ფაილები.

ნაბიჯი 5: როგორც კი მოიშორებთ მავნე პროგრამას, თქვენ დაგჭირდებათ, რომ აღადგინოთ (თქვენი სარეზერვო ასლებიდან) ან გადააყენოთ ნებისმიერი დაზიანებული ფაილი ან პროგრამული უზრუნველყოფა.

c. პროგრამული უზრუნველყოფის განახლებები

წესი #11: პროგრამული უზრუნველყოფის განახლებები არის არსებითად მნიშვნელოვანი. დარწმუნდით, რომ ჩართული გაქვთ ავტომატური განახლებები როგორც თქვენს კომპიუტერზე, ასევე მობილურ ტელეფონზე.

- თუ თქვენ Windows-ის ძველი ვერსია (7 ან 8) გაქვთ, საჭიროა განახლების პარამეტრების დაყენება ნაგულისხმევად (as default) (ე.ი. ჩართეთ ავტომატური განახლებები). იმ შემთხვევაში, თუ სისტემა განახლებული ვერსიის დაყენებას გთხოვთ, თქვენ უნდა მისცეთ მას ამის საშუალება. Windows 10-ში ადვილად ვერ გამორთავთ განახლებებს (თქვენ შეგიძლიათ გადაავადოთ ისინი მხოლოდ Pro ვერსიაში, რომლის გამოყენებას არ გირჩევთ).
- Mac: სისტემა ავტომატურად ამოწმებს განახლებებს Mac App Store აპლიკაციის მეშვეობით. Apple-ი ყოველთვის საუკეთესო მხარდაჭერას უზრუნველყოფს მხოლოდ macOS-ის უახლეს ვერსიაში. ჩართეთ ავტომატური განახლებები: Mac/About this Mac/Updates/Advanced.
- Mobile OS: რეგულარულად შეამოწმეთ განახლებები სისტემის პარამეტრებში და ყოველთვის განახლებული ვერსია გამოიყენეთ. iPhone-ებისათვის, გირჩევთ iVerify აპლიკაციას, რომელიც რამდენიმე ნაბიჯად მიგითითებთ ყველა საჭირო უსაფრთხოების ზომას.
- ნაგულისხმევი ბრაუზერები (Safari, Internet Explorer, Edge, ან Chrome Android-ის მოწყობილობებში), ჩვეულებრივ,

განახლდება თვითონ ოპერაციულ სისტემასთან ერთად. მესამე მხარის ბრაუზერების, როგორებიცაა Chrome-ი ან Firefox-ი, განახლება ხდება ცალკე და ავტომატურად. თუ ბრაუზერი გთავაზობთ განახლებას, დაუყოვნებლივ უნდა განაახლოთ ის! განახლებული ვებ-ბრაუზერის ქონა ნამდვილად ინტერნეტის უსაფრთხოების ალფა და ომეგაა. ჩვენ გირჩევთ, რომ დააყენოთ აპლიკაცია "HTTPS Everywhere", რომელიც აკონტროლებს თქვენ მიერ ნანახი ვებგვერდების უსაფრთხოებას.

d. სწორად როგორ დაბლოკოთ და განბლოკოთ მობილური მოწყობილობები

წესი #12: მნიშვნელოვანია ციფრული ან სხვა კოდის გამოყენება მოწყობილობის განსაბლოკად (პაროლი მინიმუმ 22 სიმბოლოთი). იმ შემთხვევაში, თუ მოწყობილობას თითის ანაბეჭდის სკანერი აქვს, გააქტიურეთ ის.

- ასევე მნიშვნელოვანია თქვენს ლეპტოპზე პაროლის დაყენება, რათა დაიბლოკოს და მოითხოვოს პაროლის შეყვანა ყოველ ჯერზე, როდესაც თქვენ დახურეთ ის და ხელახლა ჩართეთ. დაბლოკეთ კომპიუტერი ყოველთვის, როდესაც ტოვებთ მას, თუნდაც ცოტა ხნით (დააჭირეთ ღილაკებს Windows + L).
- შეიძინეთ ეკრანის დამცავი, რომელიც ეკრანზე გამოსახულების მხოლოდ სწორი კუთხით ნახვის საშუალებას გაძლევთ და არ აძლევს საშუალებას უცნობ პირებს, ნახონ, თუ რას წერთ ან რას აკეთებთ სხვა კუთხით შეხედვისას. როდესაც საქმე სენსიტიურ მონაცემებთან გაქვთ, ყურადღება მიაქციეთ თქვენს პოზიციას ფანჯარასთან მიმართებაში. პაროლების და სხვა მონაცემების მოსაპოვებლად საუკეთესო გზა ფანჯრებში შეხედვაა.

წესი #13: როგორც წესი, მოწყობილობის პარამეტრებში არის ფუნქცია, რომლის მეშვეობითაც წაშლით ყველა მონაცემს, თუ გაკეთებული იყო განბლოკვის რამდენიმე წარუმატებელი მცდელობა. გირჩევთ, რომ აღნიშნული ფუნქცია ჩართული გქონდეთ. გარდა ამისა, სასურველია, რომ SIM-ბარათი პაროლით იყოს დაცული, რათა შეუძლებელი იყოს მისი სხვა ტელეფონში გამოყენება.

წესი #14: აუცილებელია, რომ ტელეფონის თვალყურის დევნების ფუნქცია გააქტიურებული გქონდეთ. iOS-ის შემთხვევაში, ჩართეთ ფუნქცია „იპოვე ჩემი iPhone" (აქ თქვენ შეგიძლიათ იხილოთ დამატებითი ინსტრუქციები. Apple ასევე გიხსნით, თუ როგორ უნდა მოიქცეთ იმ შემთხვევაში, თუ თქვენი iPhone დაიკარგება ან ვინმე მოგპარავთ). თუ თქვენ იყენებთ „Android" ოპერაციულ სისტემას, დაგჭირდებათ Android Device Manager-ის დაყენება და აქტივაცია.

- მოწყობილობის დაკარგვა ან მოპარვა: დაუყოვნებლივ გახსენით აპლიკაცია სხვა მოწყობილობაზე ან ინტერნეტში (Android Device Manager / iCloud), შედით თქვენს ანგარიშზე და შეეცადეთ განსაზღვროთ თქვენი მოწყობილობის ადგილმდებარეობა. ამ ინსტრუმენტების გამოყენებით, ასევე შეგიძლიათ უსაფრთხოდ წაშალოთ ყველა მონაცემი, რომელიც თქვენს მოწყობილობაზე ინახება, იმ შემთხვევაშიც კი, თუ იმ მომენტში ადგილმდებარეობის განსაზღვრა შეუძლებელია – მონაცემები წაიშლება მაშინ, როდესაც მოწყობილობა ინტერნეტთან იქნება დაკავშირებული.

წესი #15: Apple-ის მოწყობილობებს ასევე აქვთ ფუნქცია, რომელსაც ჰქვია „Activation Lock". თუ თქვენ გაქვთ „იპოვე ჩემი iPhone" ფუნქცია, ჩართეთ ის და წაშალეთ მოწყობილობის მონაცემები მისი გამოყენებით, ის მაინც დაკავშირებული იქნება თქვენს ანგარიშთან, რაც ნიშნავს იმას, რომ ქურდი ვერ გამოიყენებს ან გააქტიურებს მას, რაც არ მისცემს მას საშუალებას, მოწყობილობა შავ ბაზარზე გაყიდოს. მოწყობილობას კავშირი ექნება თქვენს ანგარიშთან მანამ, სანამ თქვენ ფიზიკურად არ შეიყვანთ პაროლს ან ახალი მფლობელი არ გაიგებს მას – რაც ორფაქტორიან ავთენტიფიკაციასთან კომბინაციაში ყოვლად შეუძლებელია.

- Android: თუ თქვენ ჩართული გაქვთ Android Device Manager-ი, უნდა გქონდეთ წვდომა უსაფრთხოების ყველა იმ ფუნქციაზე, რომლებიც თქვენს ტელეფონს აქვს.
- სერვისები, როგორებიცაა „იპოვე ჩემი iPhone" ან „Android Lost" ასევე გაძლევთ საშუალებას დისტანსიურად შეხვიდეთ თქვენს მოწყობილობაში და მისი დაკარგვის ან მოპარვის შემთხვევაში, წაშალოთ მასში შენახული ყველა მონაცემი.

წესი #16: აგრეთვე მნიშვნელოვანია სიფრთხილე გამოიჩინოთ, როდესაც მობილურ მოწყობილობებზე Wi-Fi-ს ან Bluetooth-ს იყენებთ. აღნიშნული სერვისები ყოველთვის უნდა იყოს გამორთული, როდესაც არ იყენებთ. გარდა ამისა, მინიმუმამდე დაიყვანეთ იმ აპლიკაციების რაოდენობა, რომლებსაც წვდომა ექნებათ ინფორმაციაზე თქვენი ადგილსამყოფელის შესახებ. როგორც წესი, ეს შეიძლება იყოს საქაღალდეში „Settings/Applications/Accesses" (პარამეტრები/აპლიკაციები/წვდომის წერტილები). გადახედეთ ყველა წვდომის წერტილს და განსაზღვრეთ მათი შესაბამისობა, ხოლო შემდეგ წაშალეთ ყველა ზედმეტი. სიფრთხილე გვმართებს, როდესაც "hands-free" Bluetooth მოწყობილობებს (პრინტერები, ყურსასმენები) ვიყენებებთ, რამდენადაც ისინი უსაფრთხოების დამატებით რისკს წარმოადგენენ. გირჩევთ ე.წ. "დამტენის კონდომის" შეძენას, რომელიც მოგცემთ გარანტიას იმისა, რომ თქვენს მოწყობილობაში მხოლოდ ელექტროენერგია მიედინება. მოწყობილობაში ამ ფორმით შეღწევა ძალიან ადვილია, თუ ამის საფრთხე გათვალისწინებული არ გაქვთ.

წესი #17: თქვენს მობილურ მოწყობილობაზე კამერა და მიკროფონი შეიძლება გააქტიურდეს დისტანციურად. არასოდეს ატაროთ თქვენი სმარტფონი ისეთ ადგილებში, სადაც ის შეიძლება გამოყენებულ იქნას მოწინააღმდეგის მიერ სენსიტიური ინფორმაციის მოსაგროვებლად. კონფიდენციალური (სენსიტიური) შეხვედრების დროს შეინახეთ თქვენი მობილური ტელეფონები მოშორებით ან, თუ ტექნიკურად შესაძლებელია, ამოიღეთ აკუმულატორი. იდეალურ შემთხვევაში, თქვენი ელექტრონული მოწყობილობები უნდა ჩაიდოთ ჩანთაში, თქვენგან დაახლოებით 7-10 მეტრის მოშორებით. ამ გზით, თქვენ გექნებათ საშუალება, რომ თვალი ადევნოთ მას, მაგრამ მოწყობილობები ვერ "მოუსმენენ" თქვენს საუბარს. კამერის დაფარვის გარდა, გირჩევთ, რომ მთლიანად გამორთოთ თქვენი კომპიუტერის კამერა და ჩამოტვირთოთ აპლიკაცია "Oversight", რომელიც თვალყურს ადევნებს თქვენი კამერისა და მიკროფონის შეუსაბამო გამოყენებას.

წესი #18: დაფარეთ თქვენი ლეპტოპის ვებ-კამერა და მხოლოდ მაშინ მოიხსენით საფარი, როცა არსებობს ამის საჭიროება. იგივე თქვენს მობილურ ტელეფონს ეხება – დაფარეთ კამერა და მხოლოდ მაშინ მოიხსენით, როცა დაგჭირდებათ.

e. სარეზერვო ასლების შექმნა და საგანგებო პროტოკოლი (მოწყობილობის დაკარგვის/მოპარვის შემთხვევაში))

წესი #19: გირჩევთ, რომ თქვენი პირადი და სამსახურებრივი დოკუმენტების სარეზერვო ასლები შექმნათ დაშიფრულ გარე მყარ დისკზე, რომელიც უსაფრთხო ადგილას შეინახეთ სახლში და ხაზგარეშე რეჟიმში. კომპანია „iStorage" იაფ და კარგად დაშიფრულ გარე მყარ დისკებს ჰყიდის. რეკომენდირებულია ძალიან სენსიტიური მონაცემების იზოლირებულ სუფთა კომპიუტერზე შენახვა, რომელიც არასოდეს უერთდება ინტერნეტს. ჩვენ გირჩევთ, რომ პერსონალური კალენდრის სარეზერვო ასლი შექმნათ (იდეალურ შემთხვევაში, Google-ზე), რომელიც შეიძლება გამოგადგეთ წლების წინ მომხდარი მოვლენების გადასამოწმებლად.

წესი #20: არსებობს უამრავი აპლიკაცია დისკის დასაშიფრად, როგორც ფასიანი, ასევე უფასო. ხშირად რეკომენდირებული აპლიკაციაა VeraCrypt-ი.

წესი #21: თქვენ მხოლოდ უნიკალური და შეუნაცვლებელი დოკუმენტების სარეზერვო ასლების შექმნა გჭირდებათ. უმრავლეს შემთხვევაში, ეს არის რამდენიმე ასეული მეგაბაიტი. დარწმუნდით, რომ როგორც მინიმუმ თვეში ერთხელ ქმნით სარეზერვო ფაილებს.

f. მოწყობილობის დაკარგვის ან მოპარვის შემთხვევაში

ნაბიჯი 1: გადაამოწმეთ მოწყობილობის ადგილსამყოფელი თქვენ მიერ არჩეული თვალყურის დევნების სერვისის გამოყენებით. თუ თქვენი ტელეფონი ან ტაბლეტი სკოლაში, სამსახურში ან კაფეში დატოვეთ, დაუკავშირდით მათ პერსონალს და რაც შეიძლება მალე დაიბრუნეთ თქვენი მოწყობილობა. მსგავსი სცენარი მნიშვნელოვან რისკს არ შეიცავს.

ნაბიჯი 2: თუ თქვენი მოწყობილობის ადგილმდებარეობა დაფიქსირდა ადგილებში, სადაც არ წასულხართ ან როდესაც ხედავთ, რომ ის მოძრაობს, კარგი იქნება დაუყოვნებლივ დაუკავშირდეთ პოლიციას და ინფორმაცია მიაწოდოთ მოწყობილობის ადგილსამყოფელის შესახებ. სწრაფად მოქმედება მნიშვნელოვანია, რამდენადაც მოწყობილობის ადგილმდებარეობის ნახვა შესაძლებელია იქნება მხოლოდ მანამ, სანამ მისი აკუმულატორი არ დაჯდება ან სანამ ინტერნეტ-კავშირი არ გაითიშება.

ნაბიჯი 3: თუ თქვენ ათვითცნობიერებთ, რომ მოწყობილობაზე განსაკუთრებით სენსიტიურ ინფორმაციას ინახავთ, მაგრამ ამა თუ იმ მიზეზის გამო არ იმოქმედეთ წინა თავებში მოცემული რეკომენდაციების მიხედვით, გირჩევთ, რომ მაშინვე დისტანციურად წაშალოთ მონაცემები თქვენს მოწყობილობაზე.

ნაბიჯი 4: დაუყოვნებლივ შეცვალეთ ყველა თქვენი ანგარიშის პაროლი.

წესი #22: თქვენი მოწყობილობის დაკარგვის ან მოპარვის შემთხვევაში, ყოველთვის გახსოვდეთ, რომ ჯობია დაკარგოთ დასრულებული სამუშაოს 14 დღე, ვიდრე საფრთხეში ჩააგდოთ თქვენს მოწყობილობაში შენახული მონაცემები. მეტიც, აღნიშნულის უგულებელყოფით, თქვენ შეიძლება ასევე საფრთხეში ჩააგდოთ თქვენი დამსაქმებლის მონაცემები, რომლებიც ინახება ქლაუდ სერვერებზე. იმ შემთხვევაში, თუ არ გაქვთ შესაძლებლობა თან იქონიოთ თქვენი მობილური (თუ საჭიროა სათავსოში შენახვა), გამოიყენეთ ერთჯერადი პარკები ჩამკეტით, რათა დარწმუნდეთ, რომ მათ არავინ ახლოს ხელი. მათი სახელია „უსაფრთხოების კონვერტები" (Security envelopes), რომელთა შეძენა შესაძლებელია EuroSeal.cz-ზე.

<u>სოციალური მედიის უსაფრთხოება</u>

წესი #23: ყურადღებით მოიქეცით Facebook-ზე თქვენი კონფიდენციალურობის პარამეტრების არჩევისას – გახადეთ თქვენი პოსტები ხილვადი მხოლოდ თქვენი მეგობრებისათვის. თქვენ შეგიძლიათ კონკრეტული შინაარსის მქონე სხვადასხვა ჯგუფები შექმნათ, სადაც თქვენს მეგობრებს დაიმატებთ. დარწმუნდით, რომ თქვენი დასტურის გარეშე თქვენს გვერდზე არ გამოჩნდეს პოსტები, რომლებზეც მონიშნული ხართ. ქვემოთ შეგიძლიათ იხილოთ დეტალური გზამკვლევი. გამოტოვეთ მოცემული წესები, თუ თქვენი Facebook-პროფილი არის საჯარო.

წესი #24: გონივრული იქნება, თუ დამალავთ თქვენს საცხოვრებელ მისამართს, ტელეფონის ნომერს, ელექტრონული ფოსტის მისამართსა და სხვა მონაცემებს (ან არასოდეს შეიყვანოთ ისინი, Facebook ხშირად მას მესამე პირებს ჰყიდის). გადადით „ჩემს შესახებ" განყოფილებაში Facebook-ზე – წაშალეთ თქვენი მისამართი და აირჩიეთ შესაბამისი აუდიტორია თქვენი ელექტრონული ფოსტის მისამართისა და ტელეფონის ნომრისათვის -"მხოლოდ მე", რათა არავინ ნახოს. შეხედეთ, თუ როგორ გამოიყურება თქვენი პროფილი მეგობრების ან უცნობის თვალით „ნახეთ როგორც" ფუნქციის გამოყენებით. რათა დარწმუნდეთ, „დაგუგლეთ" თქვენი ელექტრონული ფოსტა, სახლის მისამართი და ტელეფონის ნომერი და ნახეთ სად არის ხელმისაწვდომი აღნიშნული ინფორმაცია და სად შეგიძლიათ წაშალოთ. აღნიშნული პროცედურა ასევე უნდა გაიმეოროთ თქვენი ოჯახის წევრებისთვისაც.

წესი #25: შეზღუდეთ თქვენი პროფილის მოძებნის შესაძლებლობა და მონიშნეთ „მხოლოდ მეგობრები". ყოველთვიურად წაშალეთ ყველა თქვენი Facebook-მიმოწერის კონტენტი. იმ შემთხვევაში, თუ ვინმე პროფილს მოგპარავთ, ის ვერ მოიპოვებს სენსიტიურ მონაცემებს თქვენი პირადი მიმოწერიდან.

წესი #26: არ მისცეთ საშუალება Facebook-ის გარდა სხვა საძიებო სისტემებს, რომ თქვენს პროფილზე წვდომა ჰქონდეთ.

წესი #27: გამორთეთ პერსონალიზებული რეკლამები (personalized ads).

წესი #28: თუ Facebook-ს თქვენს ტელეფონზე იყენებთ, შეზღუდეთ ან გამორთეთ აპლიკაციების წვდომა თქვენს ადგილმდებარეობაზე.

About Facebook Apps

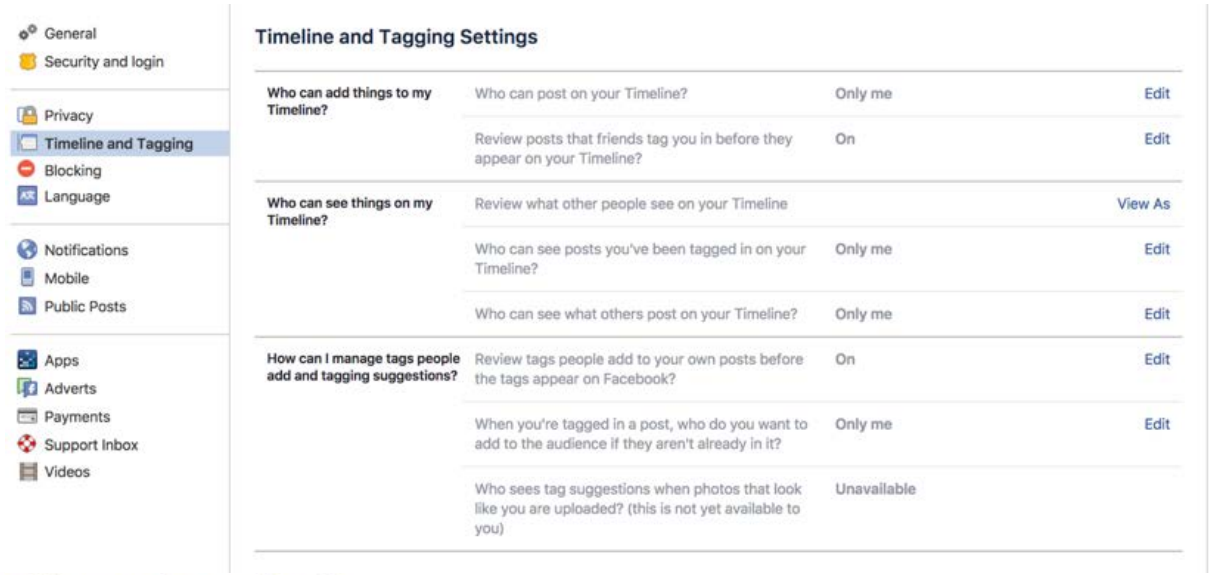
Do not login to or link third-party sites *(e.g. Twitter, Bing, LinkedIn)* using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information.

Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Edit your profile by changing all the options to Only Me (most secure) or Friends Only.

Editing Your Privacy Settings

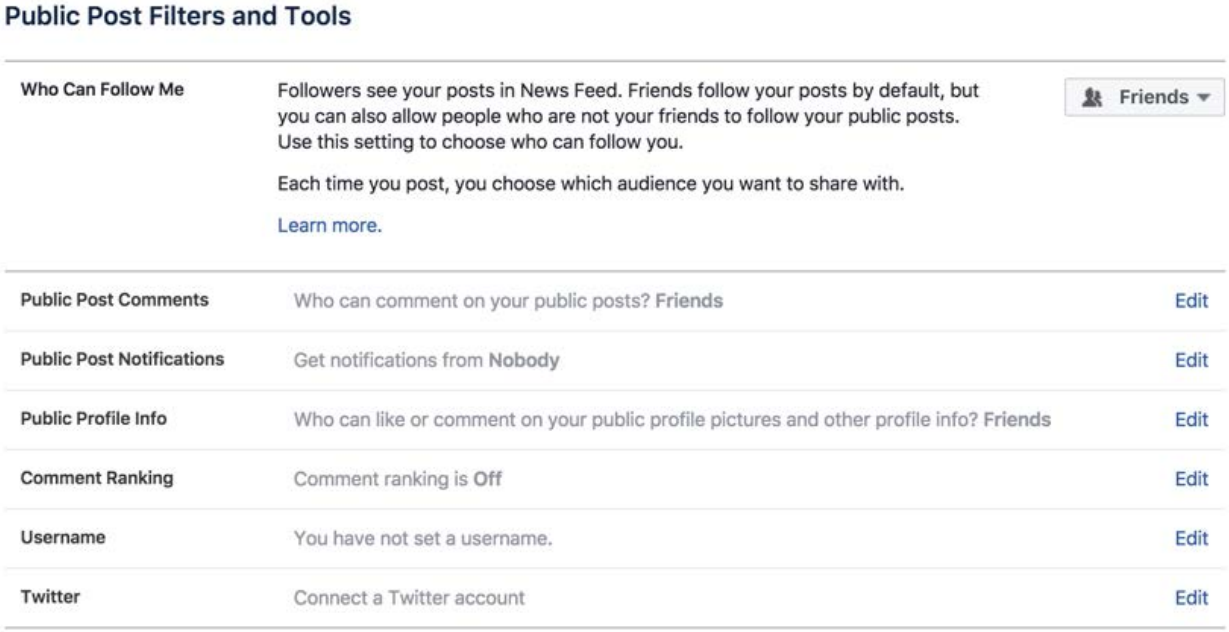
1) **Control Your Default Privacy** – Change to Friends Only
2) **How You Connect**
   a. Who can look up using your e-mail or phone number? - Friends
   b. Who can look you up using the email address or phone number you provided? - Friends
   c. Who can send you friend requests? - Friends of Friends
   d. Who can send you Facebook messages? - Friends
3) **Timeline and Tagging**
   a. Who can post on your Timeline? - Friends
   b. Who can see what others post on your timeline? - Friends
   c. Review posts friends tag you in before they appear on your timeline - On
   d. Who can see posts you've been tagged in on your timeline? - Friends
   e. Review tags friends add to your own posts on Facebook - On
   f. Who sees tag suggestions when photos that look like you are uploaded? – Friends
4) **Ads, Apps and Websites**
   a. Apps you use – Limit use of Apps
   b. How people bring your info to apps they use – Uncheck all boxes
   c. Instant personalization – Disable Personalization
   d. Public Search – Disable Public Search
   e. Ads >subpages>Ads shown by third parties – Nc one
   f. Ads >subpages>Ads and friends – No one
5) **Limit the Audience for Past Posts** – Limit the Old Posts to Friends Only
6) **Blocked People and Apps** – Here you can block certain people, events and game invites.



General
Security and login
Privacy
Timeline and Tagging
Blocking
Language
Notifications
Mobile
Public Posts
Apps
Adverts
Payments
Support Inbox
Videos

Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Only me	Edit
	Review posts that friends tag you in before they appear on your Timeline?	On	Edit
Who can see things on my Timeline?	Review what other people see on your Timeline		View As
	Who can see posts you've been tagged in on your Timeline?	Only me	Edit
	Who can see what others post on your Timeline?	Only me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Only me	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

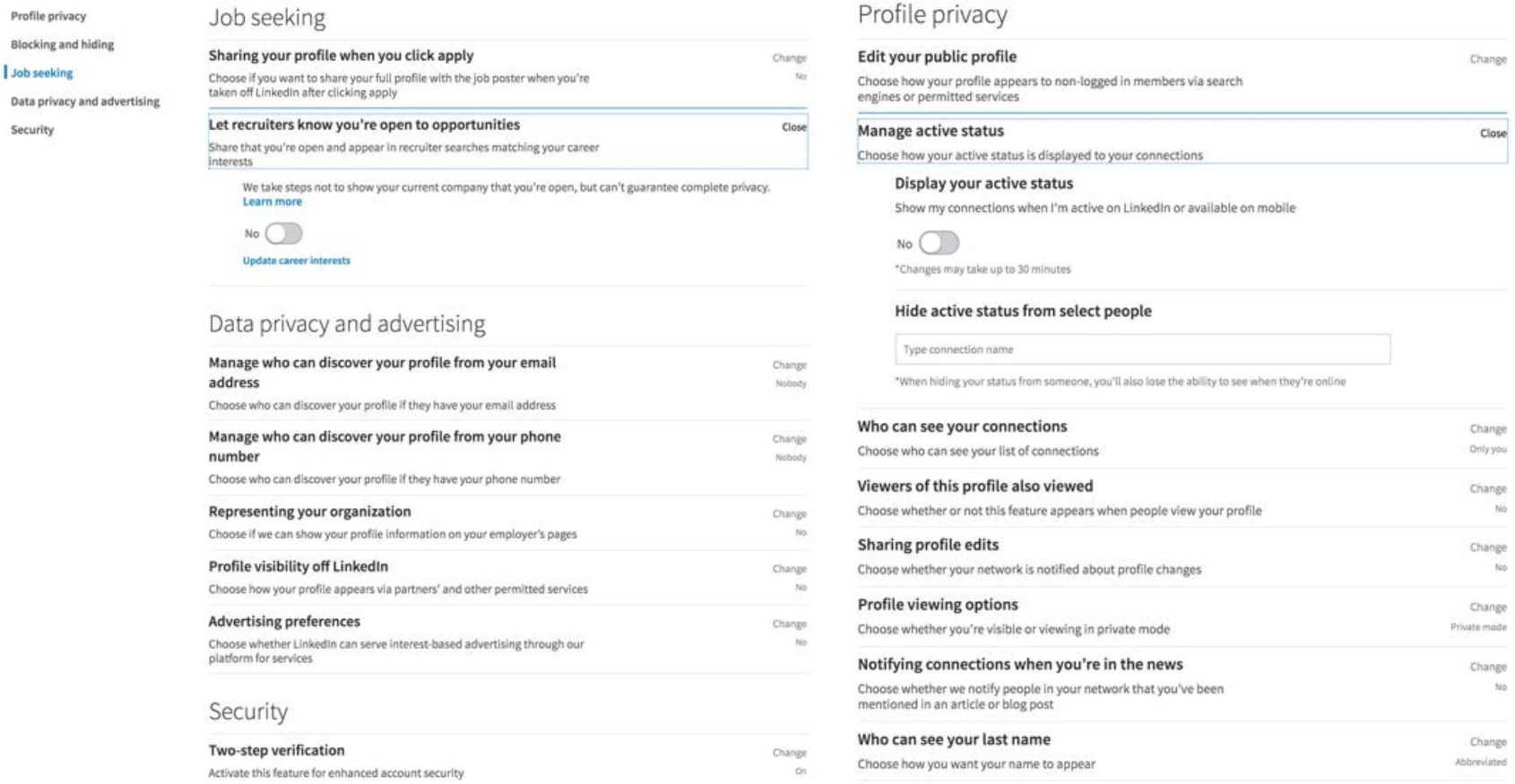


Public Post Filters and Tools

Who Can Follow Me	Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with. Learn more.	Friends
Public Post Comments	Who can comment on your public posts? **Friends**	Edit
Public Post Notifications	Get notifications from **Nobody**	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? **Friends**	Edit
Comment Ranking	Comment ranking is **Off**	Edit
Username	You have not set a username.	Edit
Twitter	Connect a Twitter account	Edit

ნაბიჯი #29: თქვენი სმარტფონით გადაღებული ფოტოები ბევრ სენსიტიურ მონაცემს შეიცავს მათი გადაღების დროისა და ადგილის შესახებ. თუ შესაძლებელია, არ გააზიაროთ ისინი პირდაპირ სოციალურ მედიაში ან გამორთეთ თქვენი ფოტოების ადგილმდებარეობა. გარდა ამისა, შეამცირეთ ფოტოს ზომა და დაარედაქტირეთ ის (რაც დააზიანებს ფოტოს მეტამონაცემებს). iVerify-ს ასევე შეუძლია თქვენი მეტამონაცემების წაშლა. სხვა შემთხვევაში, არსებობს რისკი იმისა, რომ თქვენი პროგრამული უზრუნველყოფისა და ოპერაციული სისტემის შესახებ ინფორმაცია გახდება ხელმისაწვდომი.

ნაბიჯი #30: არ შეხვიდეთ Facebook-ზე სხვა ვებგვერდების მეშვეობით – სისტემაში შესვლის აღნიშნული გზა ყოველთვის აზიარებს თქვენს მონაცემებს.



წესი #31: არ დაიმატოთ მეგობრებში მომხმარებლები, რომლებსაც არ იცნობთ. თუ წარსულში ამ წესს არ იცავდით, გადახედეთ მეგობრების ჩამონათვალს და წაშალეთ მეგობრებიდან უცნობი ადამიანები. აღნიშნული არ ეხება მათ, ვისაც საჯარო პროფილი აქვთ.

წესი#32: LinkedIn-ი ხშირად გამოიყენება პერსონალური მონაცემების მოსაგროვებლად. თუ თქვენთვის საჭიროა აღნიშნული ქსელის გამოყენება, განათავსეთ მხოლოდ საჯაროდ ცნობილი ინფორმაცია. გადაამოწმეთ, თუ რა ინფორმაცია გაქვთ აქამდე გაზიარებული LinkedIn-ზე. ყურადღებით მოიძიეთ ნებისმიერი კავშირი, რომელსაც თქვენი ოჯახისკენ ან ახლო მეგობრებისკენ მიჰყავხართ (საჯაროდ ცნობილი პირების გარდა), რამდენადაც არსებობს „დაახლოების" ("approaching") რისკი (ვინ დაგიმატებთ კონტაქტებში და როგორ გააკეთებს ამას თქვენი ნდობის მოსაპოვებლად).

a. თქვენსა და თქვენთვის ახლო ადამიანების შესახებ სენსიტიური ინფორმაციის დაცვა

წესი #33: გადაწყვიტეთ, თუ რა სახის ინფორმაციის დაცვა გსურთ. ყველაზე მნიშვნელოვანი ინფორმაციაა თქვენი საცხოვრებელი მისამართი, ინფორმაცია თქვენი ნათესავების შესახებ და თქვენი პირადი ურთიერთობების შესახებ, რომელიც თქვენმა მოწინააღმდეგემ შესაძლოა ბოროტად გამოიყენოს (რომ თქვენი ურთიერთობები კრიზისს განიცდის). დაჰყავით ინფორმაცია სამ ჯგუფად:

- საჯარო (ხელმისაწვდომია ინტერნეტში. თქვენ აქვეყნებთ მას სოციალურ მედიაში)
- პირადი (თქვენი საცხოვრებელი მისამართი, ან თქვენი პარტნიორის იდენტობა, რომელსაც მხოლოდ თქვენი მეგობრები იცნობენ)
- სენსიტიური (ხელმისაწვდომი ადამიანთა მხოლოდ იმ მცირე ნაწილისთვის, რომელსაც სრულად ენდობით)

წესი #34: გაითვალისწინეთ, რომ ყველაფერი, რასაც სოციალურ მედიაში აქვეყნებთ, „ვირტუალურად წაუშლელ" ინფორმაციად იქცევა, რომელიც თქვენს მოწინააღმდეგეებს გამოადგებათ გამოქვეყნებიდან ბევრი წლის შემდეგ. შესაბამისად, არ გამოაქვეყნოთ თქვენი სახლის, თქვენი შვილებისა და ახლო მეგობრების ან ნათესავების ფოტოები. გირჩევთ, რომ გადახედოთ ყველა თქვენს ფოტოს Facebook-ზე, Twitter-ზე და Instagram-ზე და წაშალოთ ისეთები, რომლებიც გამოავლენენ იმ ადგილების ან ადამიანების იდენტობას, რომლებიც გსურთ, რომ დაიცვათ.

წესი #35: დაუთმეთ რამდენიმე საათი თქვენს შესახებ იმ ინფორმაციის ამოსარჩევად, რომელიც, თქვენი აზრით, პირადი ან სენსიტიურია და მოძებნეთ ის Google-ის მეშვეობით, რათა დარწმუნდეთ, რომ სადმე არ გამოჩნდება. ამგვარი მოქმედებით ასევე გაიგებთ, თუ რა ინფორმაციაა საჯაროდ ხელმისაწვდომი ღია წყაროებში თქვენ შესახებ. გადადით თქვენი ახლო მეგობრების ან ნათესავების პროფილზე და სთხოვეთ, რომ წაშალონ გამოქვეყნებული ფოტოები, სადაც თქვენ ხართ გამოსახული და რომ მომავალში აღარ გამოაქვეყნონ. თუ თქვენი ნათესავების დაცვა გსურთ, არ უნდა გყავდეთ ისინი მეგობრებში (იდენტური გვარი მათ მოძებნას აადვილებს), რაც დამატებით ნაბიჯებს მოითხოვს მათი იდენტობის რეტროსპექტიული დაცვისათვის – წინამდებარე სახელმძღვანელოს ავტორები

სიამოვნებით მოგაწვდიან ინფორმაციას დამატებითი სენსიტიური ზომების შესახებ.

წესი #36: თქვენი მუდმივი საცხოვრებელი მისამართი ნაწილობრივ საჯარო ინფორმაციას წარმოადგენს, რომელიც ხელმისაწვდომია სახელმწიფოს მონაცემთა ბაზებში ან კომერციულ ხელშეკრულებებში. თუ არ გსურთ, რომ თქვენი საცხოვრებელი ადგილი ადვილად მისაგნები იყოს, შეაცვალეთ თქვენი მუდმივი საცხორებელი მისამართი, მაგალითად, თქვენი მშობლების ან სხვა ნათესავების საცხოვრებელი მისამართით. შესაძლებელია თქვენი მუდმივი საცხოვრებელი მისამართის შეცვლა კომერციულად, თქვენი ორგანიზაციის მეშვეობით.

წესი #37: გააქტიურეთ Google Alerts შეტყობინების ფუნქცია, რომელიც ელ-ფოსტაზე გამოგიგზავნით შეტყობინებებს, თუ თქვენი სახელი (ან თქვენი სახელის, თანამდებობის, ან თქვენი თანამშრომლის კომბინაცია) რომელიმე ვებსაიტზე ჩნდება. იგივე გაიმეორეთ თქვენი სახელის, დაკავებული პოზიციის ან დამსაქმებლის სხვადასხვა კომბინაციით. შედეგები არ მოიცავს სოციალურ მედიას.

b. ანონიმურობა ინტერნეტში

ინტერნეტ-სივრცეში ყველა თქვენი აქტივობა გარკვეულ ინფორმაციას ამჟღავნებს თქვენი იდენტობის შესახებ. აღნიშნული ინფორმაცია შეიძლება გაანალიზდეს, შედარდეს და გამოყენებულ იქნას თქვენი პროფილის შესაქმნელად, რამაც შეიძლება გამოააშკარაოს დიდი მოცულობის სენსიტიური ინფორმაცია ინტერნეტში თქვენი ქცევის შესახებ. მიუხედავად იმისა, რომ არ არსებობს სრული ინტერნეტ-ანონიმურობა, გირჩევთ, რომ მინიმუმამდე შეამციროთ ინფორმაციის რაოდენობა, რომელსაც თქვენს შესახებ აზიარებთ, განსაკუთრებით, თუ სენსიტიურ საქმიანობას ეწევით. ის, რაც ამჟამად შეიძლება ბანალურად მოგეჩვენოთ, ხუთი ან ათი წლის შემდეგ შეიძლება გამოყენებულ იქნას თქვენი პროფილის ფსიქოლოგიური ანალიზისთვის:

წესი #38: გამოიყენეთ DuckDuckGo (http://duckduckgo.com) როგორც თქვენი ძირითადი საძიებო სისტემა. აღნიშნული სისტემა დაშიფრულ კავშირს იყენებს და არც IP მისამართებს, არც თქვენი ძიების ისტორიას არ ინახავს. გამორთეთ ავტომატური შესვლის ფუნქცია ყველა სხვა ბრაუზერზე. მზა ფაილები (cookies): ფართოდ გამოყენებულ ბრაუზერებში (Chrome, Firefox, Internet Explorer, Safari) შეგიძლიათ გამოიყენოთ ბრაუზერის პრივატული (private/anonymous) "ფანჯრები", რომლებიც არ ინახავს მზა ფაილებს (cookies). მიუხედავად ამისა, თქვენი IP მისამართის იდენტიფიცირება მაინც ხდება, ხოლო თქვენს ინტერნეტ პროვაიდერს შეუძლია თვალი მიადევნოს თქვენს ონლაინ აქტივობას.

წესი #39: კარგი საშუალება ანონომური და კონფიდენციალური დოკუმენტების გასაზიარებლად არის Crabgrass-ი (https://we.riseup.net/crabgrass), რომელიც საშუალებას გაძლევთ დარეგისტრირდეთ ანონიმურად და გამოიყენოთ ის თქვენს გუნდში დოკუმენტების გასაზიარებლად.

წესი #40: თქვენი ონლაინ იდენტობის დასაფარად, გთავაზობთ VPN-ის ფასიანი ვერსიის გამოყენებას. გირჩევთ VPNSecure.me-ს, Proton VPN-ს ან Avast-ს არა მხოლოდ თქვენს ლეპტოპზე, არამედ თქვენს ტელეფონზე ან ტაბლეტზეც.

თუკი ოდესმე უკავშირდებით დაუცველ Wi-Fi-ს, თქვენს ინტერნეტ აქტივობაზე თვალყურის დევნება ძალიან ადვილი ხდება. არასოდეს გამოიყენოთ დაუცველი Wi-Fi-ი, როდესაც საქმე სენსიტიურ ინფორმაციას ეხება. არასოდეს განაახლოთ პროგრამული უზრუნველყოფა დაუცველი Wi-Fi-ის გამოყენებით. სამ თვეში ერთხელ შეცვალეთ თქვენი სახლის Wi-Fi-ის პაროლი. გამოიყენეთ VPN-ის „Kill Switch" ფუნქცია, რომელიც სუსტი კავშირის შემთხვევაში, ავტომატურად გამორთავს თქვენს ინტერნეტ-კავშირს, რათა დარწმუნდეთ, რომ VPN-ით ხართ შესული.

წესი #41: არსებობს მხოლოდ ერთადერთი გზა ქსელში ანონიმურობის მაღალი დონის მისაღწევად - სპეციალური ვებ ბრაუზერის, Tor-ის გამოყენება. ჩვენ არ გირჩევთ მისი ყოველდღიური საქმიანობისთვის გამოყენება – ის საკმაოდ ნელია. გამოიყენეთ ბრაუზერი მხოლოდ მაშინ, როდესაც გინდათ დარწმუნდეთ, რომ თქვენი ონლაინ აქტივობის გარკვეული ნაწილი არ იქნება იდენტიფიცირებული (ეს არ გულისხმობს მხოლოდ უკანონო ქმედებებს; თქვენ შეიძლება მოგინდეთ თავი დაიცვათ პოლიტიკურად სენსიტიური წინადადებებისა და ადამიანებთან კომუნიკაციის გამო, რომელიც არ გინდათ, რომ გასაჯაროვდეს და ა.შ.). თუ თქვენ იყენებთ Tor-ს, არ დააყენოთ პლაგინები (plug-ins) ან ჩამოტვირთოთ ტორენტები ერთდროულად. ასევე რეკომენდირებულია, რომ არ გახსნათ დოკუმენტები Tor-ის საშუალებით (.doc და .pdf ფაილების შემთხვევაშიც კი). თუ თქვენ უნდა იმუშაოთ დოკუმენტებზე, დროებით გამორთეთ ინტერნეტი თქვენს კომპიუტერზე.

<u>კომუნიკაციის დაცვა</u>

a. კომუნიკაციის დაშიფრვა

თუ სენსიტიურ ინფორმაციას ხელით წერთ ბლოკნოტში, გირჩევთ, რომ ყოველდღიურად გაანადგუროთ ის (დააქუცმაცეთ პატარ-პატარა ნაწილებად და უნიტაზში ჩაუშვით). ასე, დარწმუნდებით, რომ არ დაგავიწყდებათ ბლოკნოტი, რომელშიც მნიშვნელოვანი ჩანაწერები გაქვთ გაკეთებული და არ ჩააგდებთ ინფორმაციას საფრთხეში.

კომუნიკაციის ყველაზე ნაკლებად უსაფრთხო გზებია:

- <u>სატელეფონო ზარები, ტექსტური შეტყობინებები:</u> პროვაიდერები ინახავენ სატელეფონო ზარებისა და ტექსტური შეტყობინებების ჩანაწერებს და ხშირად შეუძლიათ მესამე მხარისთვის მათი გადაცემა (გარკვეული პირობებით). თქვენი ზარებისა და ტექსტური შეტყობინებებისათვის თვალყურის დევნება ადვილია კომერციულად ხელმისაწვდომი ტექნოლოგიების გამოყენებით.
- <u>ელექტრონული წერილები</u> ინახება თქვენი პროვაიდერის სერვერებზე, რაც მათ ხელმისაწვდომს ხდის ყველასთვის, ვინც იცის თქვენი ელ. ფოსტის ანგარიშის პაროლი ან თავად პროვაიდერისთვის. იგივე ეხება Facebook-სა და Twitter-ს. დაუშიფრავი ელექტრონული წერილი იგივეა, რაც საფოსტო ბარათის ფოსტით გაგზავნა – ყველას, ვისაც სურს, შეუძლია მისი წაკითხვა.

წესი #41: შეტყობინებებისათვის ყველაზე უსაფრთხო დაშიფრული აპლიკაცია არის Signal-ი, რომლის საშუალებითაც

ასევე შეგიძლიათ ზარის (მაგრამ არა ჯგუფური ზარების) გაკეთება. თუ თქვენ იყენებთ Signal-ს, მნიშვნელოვანია, რომ კონფიდენციალურობის პარამეტრებში ყველაფერი ჩართული გქონდეთ –კოდური ფრაზის შექმნისა და შეტყობინებების რეგულარული წაშლის ჩათვლით (ჩვენ გირჩევთ ერთდღიან ინტერვალს). ჩვენ არ გირჩევთ WhatsApp-ის ან Skype-ის გამოყენებას სენსიტიური ინფორმაციის გადასაცემად ან მისაღებად. მნიშვნელოვნად სენსიტიური მონაცემებისთვის გირჩევთ Wickr Me-ის გამოყენებას. არ გამოიყენოთ Viber-ი ან Telegram-ი. როდესაც ზარებს დაშიფრული აპლიკაციის საშუალებით აკეთებთ, გაითვალისწინეთ თქვენი გარემო. არასოდეს ილაპარაკოთ სენსიტიური ინფორმაციის შესახებ საზოგადოებრივ ტრანსპორტში, უცნობ პირთან მანქანაში ან სხვა ადამიანებთან ერთ ოთახში ყოფნის დროს. საუკეთესო გამოსავალია გარეთ გასეირნება.

წესი #42: ყველაზე უსაფრთხო აპლიკაცია დაშიფრული წერილებისათვის არის ProtonMail-ი, იმ პირობით, რომ მას ორივე მხარე იყენებს. ProtonMail-ი ხელმისაწვდომია iOS-ზე, Android-ზე, აგრეთვე ვებ-გვერდზე. რეკომენდირებულია, რომ ჩამოტვირთოთ Proton Bridge-ის ფასიანი ვერსია, რამდენადაც ის საშუალებას გაძლევთ Proton Mail-ი თქვენი კომპიუტერის ელ. ფოსტის კლიენტში დააინსტალიროთ. არ დაგავიწყდეთ ორფაქტორიანი ავტორიზაციის ჩართვა. გაწმინდეთ ProtonMail-ი სამ თვეში ერთხელ ყველა მიღებული და გაგზავნილი ელ. წერილების წაშლის გზით. რამდენადაც ProtonMail-ისათვის გვჭირდებათ მეორე სარეზერვო ელ. ფოსტა, გირჩევთ, რომ შექმნათ ცალკე (შეიძლება იყოს უფასო) ProtonMail-ი სუპერ ძლიერი პაროლით (40 სიმბოლოთი), რომელიც იქნება გამოყენებული როგორც სარეზერვო ელ. ფოსტა ყველა დანარჩენი პროფილისათვის – Facebook-ი, Twitter-ი, LinkedIn-ი, Instagram-ი, საბანკო ანგარიშები.

<u>მონაცემთა უსაფრთხოება</u>

ყოველი გაზიარებული საქაღალდე (Dropbox-ში) იმდენად არის დაცული, რამდენადაც გუნდის ყველაზე ნაკლებად დაცული წევრი.

რეკომენდირებული iPhone-ის პარამეტრები:

- Settings>Notifications> გადაამოწმეთ ყველა აპლიკაცია და დარწმუნდით, რომ შეტყობინებები არ იქნება ხელმისაწვდომი დაბლოკილ(კოდდადებულ) ეკრანზე
- Settings>privacy>location services>
  - >share my location – გამორთეთ (დააყენეთ „off“-ზე)
  - გადაამოწმეთ ყველა აპლიკაცია და განსაზღვრეთ, თუ როდის გჭირდებათ GPS-ი, „როდესაც იყენებთ“ თუ „არასდროს“. დარწმუნდით, რომ არაფერზე გაქვთ მონიშნული „ყოველთვის“ („always“)
  - დარწმუნდით, რომ აირჩიეთ „არასდროს“ კამერისთვის (წინააღმდეგ შემთხვევაში, თქვენს სურათებზე მონიშნული იქნება მათი გადაღების ადგილი); ყველა სოციალური მედიის აპლიკაციისთვის (Twitter-ი, Facebook-ი, Instagram-ი)

- >systems services – ყველა გამორთულია, „Emergency SOS“-ის და (არასავალდებულო) „იპოვე ჩემი iPhone“-ის გარდა
- >frequent locations – „წაშალე ისტორია“ და „off“-ზე გადართე (გამორთე)
- Product improvement – ყველა გამორთე („off“)

• Settings>privacy>
- Diagnostics & Usage – „არ გააგზავნო “
- Advertising – „Reset Advertising Identifier“ და „Limit Ad Tracking“ – ჩართე („on“)

a. დისკის დაშიფრვა

წესი #43: დაშიფრეთ თქვენი დისკი:

- macOS: შეიცავს დისკის დაშიფრვის პროგრამას - FileVault-ს – მას შემდეგ რაც მას ჩართავთ, პროგრამა აღმდგენ გასაღებს შემოგთავაზებთ (რომელიც უსაფრთხოდ შეგიძლიათ შეინახოთ Apple-ის სერვერებზე), ამის შემდეგ დაშიფრეთ მთელი დისკი. მომდევნო დეშიფრაცია ფონური პროცესია, რომელიც შეუმჩნეველია მომხმარებლისათვის და არ ანელებს სისტემის მუშაობას.
- Windows-ი: დაშიფრვის ტექნოლოგია BitLocker-ი Windows-ის მხოლოდ პროფესიონალური ვერსიების შემადგენელი ნაწილია. აპლიკაციები, როგორებიცაა VeraCrypt-ი ან CipherShed-ი კარგ ალტერნატივას წარმოადგენს იმ მომხმარებლებისათვის, ვინც BitLocker-ის გარეშე ვერსიებს იყენებს.
- მობილური ტელეფონებს და ტაბლეტებს Androids 5.0-ით (Lollipop) და უფრო ახალი ვერსიებს ჩვეულებრივ აქვთ დაშიფრვის ფუნქცია, თუმცა, ბევრ შემთხვევაში ის აუარესებს მოწყობილობის მწარმოებლურობას, რაც არაკომფორტულია მომხმარებლისათვის. შესაბამისად, ასეთ შემთხვევებში ჩვენ გირჩევთ, რომ დაშიფრვის ფუნქცია გამორთული დატოვოთ, იმ პირობით, რომ მომხმარებელი შემდეგ რეკომენდაციებს დაიცავს.

b. დაშიფრვა და მოსახსნელ დისკებზე შენახული მონაცემების უსაფრთხო წაშლა

წესი #44: USB ფლეშ დრაივები (flash drives): Mac-ის შემთხვევაში, საჭიროა მაძიებელში დისკის ნიშანზე მარჯვენა დაწკაპუნება და ფუნქცია Encrypt-ის (დაშიფრვა) არჩევა. სხვა კომპიუტერთან მისი შეერთებისას, უბრალოდ პაროლი შეგყავთ. თუ თქვენი Windows-ის ვერსია შეიცავს BitLocker-ს, დისკების დაშიფრვა შეგიძლიათ საკონტროლო პანელის სექცია BitLocker-ში ან უბრალოდ მოსახსნელი დისკის ნიშანზე მარჯვენა დაწკაპუნებით. თუ თქვენი Windows-ის ვერსია არ შეიცავს BitLocker-ს, თქვენ შეგიძლიათ გამოიყენოთ ზემოაღნიშნული აპლიკაცია VeraCrypt-ი, რომელსაც იგივე ფუნქცია აქვს. არასოდეს შეუერთოთ უცნობი USB flash drive თქვენს მოწყობილობას, მაშინაც კი, როდესაც თქვენი მეგობრისაა – თქვენ არ იცით, ზრუნავს თუ არა ის უსაფრთხოებაზე. დააყენეთ USB software Safeguard-ი, რომელიც მხოლოდ შემოწმებულ ფლეშ დრაივებს გახსნის. უცნობი ფაილებისათვის გამოიყენეთ აპლიკაცია Sandbox -ი.

წესი #45: დისკზე მონაცემების ჩვეულებრივად წაშლა არ ხდის მათ მიუწვდომელს– აქედან გამომდინარე, საჭიროა

უსაფრთხო წაშლის განხორციელება, რაც უფრო დიდ დროს მოითხოვს, მაგრამ შეგეძლებათ თქვენი დისკი ნებიმსიერ პირს მისცეთ:

- MacOS: თქვენ შეგიძლიათ გამოიყენოთ სისტემური აპლიკაცია Disk Utility (Erase disk-ის სექცია უსაფრთხო წაშლის ღილაკს მოიცავს). გამოიყენეთ აპლიკაცია Eraser-ი.
- Windows: ამჟამად, Windows-ს არ გააჩნია უსაფრთხო წაშლის ფუნქცია თავის ძირითად კონფიგურაციაში. თუმცა, CCleaner-ის უფასო ვერსიას შეუძლია უსაფრთხოდ წაშალოს მონაცემები მოსახსნელი დისკებიდან.

პირადი უსაფრთხოება

წესი #46: არ არის რეკომენდირებული შენობის შესასვლელთან კარის ზარზე სახელის მითითება. თუ ამის გაკეთება აუცილებელია, მაშინ თქვენი სახელი არ უნდა მიუთითოთ უშუალოდ თქვენი ბინის კარზე.

წესი #47: თუ სახლიდან დიდი ხნით მიდიხართ, არ დააანონსოთ ამის შესახებ საჯაროდ და დარწმუნდით, რომ სოციალურ ქსელებში თქვენი პოსტები თქვენს ადგილსამყოფელს არ აჩვენებს. სამოგზაურო სურათები მხოლოდ მაშინ გამოაქვეყნეთ, როდესაც სახლში დაბრუნდებით. ტაქსის ან Uber-ის შეკვეთისას, რეკომენდირებულია, რომ აღნიშნული არ გააკეთოთ თქვენი დასარჩენი ადგილიდან, არამედ 50 მეტრის მოშორებით მაინც. იგივენაირად მოიქეცით, როცა მანქანას ან სხვა ტრანსპორტს ტოვებთ. ადგილსამყოფელის მონაცემები თქვენს პროფილში ინახება და შეიძლება მოპოვებულ იქნას შედარებით ადვილად.

წესი #48: მოიფიქრეთ პაროლი ახლობელ ადამიანებთან ერთად, რათა შეძლონ თქვენთვის ტექსტური შეტყობინების გაგზავნა ან დარეკვა, როდესაც მათ საფრთხე დაემუქრებათ. ასეთ შემთხვევაში, დაუყოვნებლივ დარეკეთ პოლიციაში და მოძებნეთ ისინი – დარწმუნდით, რომ მათ გითხრეს თავიანთი ადგილსამყოფელის შესახებ. იგივე გააკეთეთ თქვენი ოჯახის წევრებისასთვის. თუ თქვენ ზარის გაკეთების შესაძლებლობა არ გაქვთ, შეგიძლიათ უბედურების სიგნალის (distress signal) გაგზავნა.

წესი #49: არასოდეს შეხვიდეთ დახურულ სივრცეში მარტო და უცნობ პირთან ერთად. ამის ნაცვლად, შეანელეთ ნაბიჯი, მოიქეცით ისე, თითქოს ზარს აკეთებთ ან გადაუხვიეთ სადმე და სხვა გზით წადით. თუ ნებისმიერ ადგილას თავს არაკომფორტულად გრძნობთ, დაუყოვნებლივ აიღეთ თქვენი ტელეფონი და მოიქეცით ისე, თითქოს ახლობელ ადამიანს ურეკავთ. ხმამაღლა უთხარით თქვენი ადგილსამყოფელი და, მაგალითად, „მოუყევით“, რომ თქვენთან ახლოს იმყოფება უცნაური ადამიანი და აღწერეთ მისი გარეგნობა. თითქმის ყოველთვის, ეს ხერხი მუშაობს როგორც წარმატებული შემაკავებელი. დაიწყეთ ყვირილი, ხმამაღლა. ცრუ განგაშით არაფერს კარგავთ, რასაც ვერ ვიტყვით ალტერნატივაზე.

წესი #50: იმისათვის, რომ დაახლოებით ამოიცნოთ, თუ რამდენად სერიოზულია კონკრეტული საფრთხე, დაიმახსოვრეთ ქვემოთ მოყვანილი ცხრილი. ფიზიკური ინციდენტის შემთხვევაში, ძირითადი წესია: გაიქეცი, დაიმალე, იბრძოლე.

8. KEY FINDINGS

- სამოქალაქო საზოგადოების ორგანიზაციებში კიბერუსაფრთხოების გზამკვლევების არარსებობა.
- ოპერაციული უსაფრთხოების შინაგანაწესის დაცვის მზადყოფნის არარსებობა.
- არასამთავრობო ორგანიზაციებში შესაბამისი ადამიანური რესურსების (სპეციალისტების) ნაკლებობა
- ოპარაციულ უსაფრთხოებას არ უდგებიან სერიოზულად.
- ოპერაციული უსაფრთხოების ჩვეულებრივი შეცდომები, რომლებსაც უშვებენ სახელმწიფო მოხელეები, ჟურნალისტები და არასამთავრობო სექტორი, რაც მათ მარტივ სამიზნედ ხდის
  - "ისეთი მნიშვნელოვანი არ ვარ."
  - "არალეგალურს არაფერს ვაკეთებ."
  - "ეს არ არის გასაიდუმლოებული."
- რუსული და ჩინური გავლენის წინააღმდეგ ბრძოლის სფეროში მუშაობა თქვენ სამიზნედ გხდით.
- რუსეთსა და ჩინეთს ადვილად შეუძლიათ ამ სფეროში მომუშავე ათასობით პირის შემოწმება.

9. შეჯამება

უსაფრთხოების ათი ჩვევა, რომლებიც ყველამ უნდა იცოდეს

წესები, რომელთა დაცვასაც გირჩევთ, ზემოთ არის ჩამოთვლილი. ხშირად ეს არის ნაბიჯები, რომლებიც მხოლოდ ერთხელ უნდა გადადგათ. უსაფრთხოების მხრივ თქვენი ქცევის გამოსწორების საწყისი ეტაპის გავლის შემდეგ, რეკომენდირებულია, რომ შემდეგი ყოველდღიური ჩვევები აითვისოთ და დაიცვათ რეგულარულად, ისე, როგორც იხეხავთ კბილებს ან კეტავთ თქვენი სახლის კარებს:

ჩვევა # 1: უსაფრთხო კომუნიკაციისთვის გამოიყენეთ მხოლოდ აპლიკაცია Signal-ი (შეტყობინებისთვის და ზარებისთვის), ხოლო ProtonMail-ი დაშიფრული ელექტრონული წერილებისათვის. არ ენდოთ აპლიკაციებს, როგორებიცაა: WhatsApp-ი, Facebook Messenger-ი, ან Telegram-ი უფრო სენსიტიური მიმოწერისთვის (წესები # 41 - # 42)

ჩვევა # 2: რეგულარულად წაშალეთ მონაცემები თქვენს კომპიუტერში Permanent Eraser ან Cleaner პროგრამების გამოყენებით. (წესი # 45)

ჩვევა # 3: კიბერშეტევების უმრავლესობა ხორციელდება ფიშინგის გზით. შესაბამისად, ელექტრონული წერილის ყველა თანდართული ფაილი გახსენით Sandbox-ში და გადაამოწმეთ ყველა მიღებული ლინკი virustotal.com-ის მეშვეობით. (წესი # 10)

ჩვევა # 4: არ ენდოთ არცერთ USB დრაივს, რადგან შეუძლებელია მათი უსაფრთხოების შემოწმება. შესაძლებლობის შემთხვევაში, უკეთესი იქნება მონაცემების ProtonMail-ზე გადაგზავნა. ალტერნატივის სახით, იქონიეთ ცალკე კომპიუტერი ინტერნეტ-კავშირის გარეშე, სადაც თქვენ შეგიძლიათ გახსნათ USB დრაივი. (წესი# 44)

ჩვევა # 5: კონფიდენციალური (სენსიტიური) შეხვედრების დროს შეინახეთ თქვენი მობილური ტელეფონები უსაფრთხო ადგილას. იდეალურ შემთხვევაში, თქვენი ელექტრონული მოწყობილობები უნდა ჩაიდოთ ჩანთაში დაახლოებით 7-10 მეტრის მოშორებით, ისე, რომ იყოს თქვენს მხარეს მაგრამ არ იყოს რისკი იმისა, რომ მოწყობილობები "უსმენდნენ" თქვენს საუბარს. (წესი # 17)

ჩვევა # 6: არ არის რეკომენდირებული უკაბელო კავშირის მქონე მოწყობილობების (ყურსასმენები, პრინტერები) გამოყენება. შეიძინეთ "USB კონდომები" თქვენი ტელეფონისა და კომპიუტერების დამტენებისათვის (წესი # 16).

ჩვევა # 7: როდესაც სოციალური მედიის ანგარიშებზე ინფორმაციას ან სურათებს ამატებთ, გამოაქვეყნეთ მხოლოდ ისინი, რომლების ნახვას თქვენს ოპონენტებსაც ნებას დართავდით. თუ რამეს თქვენი ოჯახისა და ნათესავების ან

თქვენი პირადი ცხოვრების შესახებ აქვეყნებთ, თქვენს ოპონენტებს შეუძლიათ შექმნან ფსიქოლოგიური პროფილი და სოციალური რუკა და გამოიყენონ აღნიშნული ინფორმაცია. (წესი # 33)

ჩვევა # 8: ყოველთვის გამოიყენეთ VPN: VPN Secure Me, Proton VPN-ი ან Avast-ი. დაიცავით „kill-switch" წესი. (წესი # 40)

ჩვევა # 9: თუ თქვენ სენსიტიური ხასიათის ჩანაწერებს ხელით აკეთებთ, გირჩევთ, რომ გადაამუშაოთ ისინი დღის განმავლობაში, ხოლო შემდეგ გაანადგუროთ ისინი (ან პატარ-პატარა ნაწილებად დაქუცმაცებას და ჩააგდეთ ნაგვის ყუთში თქვენი სახლისგან ან ოფისისგან მოშორებით).

ჩვევა # 10: დააყენეთ კალენდრის შეხსენება: სამ თვეში ერთხელ ვცვლით პაროლებს. (წესი # 1 - # 4). ჩვენ გირჩევთ, რომ თქვენი პერსონალური დოკუმენტების, ელექტრონული კალენდრის მონაცემებისა და თქვენი სამუშაო ფაილების სარეზერვო ასლები შექმნათ გარე დაშიფრულ დრაივერზე ყოველთვიურად. (წესი # 19)

დაუშიფრავი ელექტრონული წერილები არის იგივე, რაც თქვენი შეტყობინებების გამოქვეყნება საჯაროდ და რეალურ დროში

გაურთულეთ საქმე მოწინააღმდეგეებს

1. გამოიყენეთ ძლიერი VPN (Avast Secureline-ი, ProtonVPN-ი, Nord VPN-ი, ...).
2. გამოიყენეთ კარგი ანტივირუსი და Anti-ransom პროგრამული უზრუნველყოფა (Avast-ი, Eset-ი, McAfee...).
3. დაშიფრეთ თქვენი მონაცემები (VeraCrypt-ი).

არ ჩაალაგოთ ყველა კვერცხი ერთ კალათაში

1. დაიცავით ყველა თქვენი ანგარიში და პროფილი ორმაგი ავტორიზაციის მეშვეობით.
2. იქონიეთ რამდენიმე კარგად დაცული იმეილი თქვენი ანგარიშებისათვის, რათა ერთის გატეხვის შემთხვევაში, ყველაფერი ერთად არ დაიკარგოს
3. გამოიყენეთ ძლიერი პაროლები. არ გამოიყენოთ ერთი პაროლი ყველა ანგარიშისათვის.

ყოველთვის განმეორებით გადაამოწმეთ ახალი ადამიანების ვინაობა, რომლებსაც ხვდებით

1. ყოველთვის გამოიკვლიეთ (Google-ის მეშვეობით) მათი წარსული და მოკლე ცნობები მიიღეთ იმ პირებისგან, რომლებიც მას იცნობენ
2. არ შემოუშვათ უცნობი პირები თქვენს ოფისებში.

იცოდეთ, თუ რომელ საიდენტიფიკაციო ინფორმაციას იცავთ

ხომ არ არის თქვენი Facebook-ის პროფილი სავსე ინფორმაციით თქვენი პარტნიორისა და თქვენი ბავშვების შესახებ?
გააცნობიერეთ, რომ საჯარო ინფორმაცია ადვილად ხელმისაწვდომია მოწინააღმდეგეებისთვის და შეიძლება გამოყენებულ იქნას თქვენ წინააღმდეგ.