CAUCASUS OPEN SPACE

კიბერუსაფრთხოების შესაძლებლობების განვითარების ტრენინგ-კურსის სახელმძღვანელო

კიბერუსაფრთხოების შესაძლებლობების განვითარების ტრენინგ-კურსის სახელმძღვანელო

CAUCASUS OPEN SPACE

კიბერუსაფრთხოების შესაძლებლობების განვითარების ტრენინგ-კურსის სახელმძღვანელო

სახელმძღვანელო განკუთვნილია საქართველოს ადგილობრივ თვითმმართველობებში დასაქმებული თანამშრომლებისთვის და მიზნად ისახავს მათი ცნობიერების ამაღლებას ინტერნეტით სარგებლობის პოტენციური რისკების შესახებ, კიბერშესაძლებლობების განვითარებასა და კიბერმედეგობის გაძლიერებას კომპიუტერულ ინციდენტებსა და საფრთხეებთან გასამკლავებლად. სახელმძღვანელო შემუშავებულია მუნიციპალიტეტების კიბერმზაობის შეფასების შედეგად და მასალების მომზადებისას გათვალისწინებულია საქართველოში არსებული გამოწვევები, ისევე როგორც ნატო-სა და ევროკავშირის საუკეთესო გამოცდილება და მიდგომები.

სახელმძღვანელო შემუშავდა შეერთებული შტატების საერთაშორისო განვითარების სააგენტოს, დემოკრატიული მმართველობის (USAID GGI) პროექტის „კიბერუსაფრთხოების შესაძლებლობების განმტკიცება ადგილობრივ დონეზე“ ფარგლებში, რომელსაც ახორციელებს ღია სივრცე კავკასია. ანგარიშის შინაარსზე პასუხისმგებელია ღია სივრცე კავკასია (COS) და ის შესაძლოა არ ასახავდეს USAID-ის ან აშშ-ის მთავრობის შეხედულებებს.

ავტორები: ნატალია გოდერძიშვილი, ირმა პავლიაშვილი

გამოცემაზე პასუხისმგებელი პირები: თეონა მაჭარაშვილი, ირმა პავლიაშვილი

რედაქტორი/ტექ.რედაქტორი: დავით ინანეიშვილი, მაია ახალაია

დიზაინი და დაკაბადონება: თეონა ნაცვლიშვილი

თბილისი, 2021

© აკრძალულია სახელმძღვანელოში მოყვანილი მასალების გადაბეჭდვა, გამრავლება და გავრცელება კომერციული მიზნით ღია სივრცე კავკასიის ნებართვის გარეშე

წინასიტყვაობა

ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებმა თანამედროვე საზოგადოებრივი ცხოვრების საერთო სურათი რადიკალურად შეცვალა. ტექნოლოგიების განვითარებასთან ერთად, ინფორმაციულ-საკომუნიკაციო საშუალებებზე საზოგადოებისა და ბიზნესის მზარდი დამოკიდებულების, ელ-სერვისების ფართომასშტაბიანი დანერგვისა და ციფრულ ეკონომიკაზე გადასვლის კვალდაკვალ, იზრდება ტექნოლოგიებიდან მომდინარე რისკები, საფრთხეები და ინციდენტები. სოციალური ურთიერთობებისთვის ფიზიკურის პარალელურად, ციფრულმა ტრანსფორმაციამ შექმნა ახალი ვირტუალური კიბერსამყარო. მსოფლიოს მოსახლეობის დაახლოებით მესამედს აქვს ინტერნეტზე წვდომა და მონაწილეობს ვირტუალური სფეროს მიერ შემოთავაზებულ სხვადასხვა აქტივობებში. კიბერსფეროს ევოლუციამ ხელი შეუწყო ტრანსნაციონალური ეკონომიკური და სოციალური ურთიერთობების გამარტივებას, გააქტიურებას და ამავდროულად გააჩინა ახალი შესაძლებლობები კანონსაწინააღმდეგო, არალეგალური აქტივობებისთვის.

ციფრული რევოლუციის თანმდევი შედეგია კიბერუსაფრთხოება და მისი უზრუნველყოფა[1] 21-ე საუკუნის სამყაროსთვის ერთ-ერთი ყველაზე დიდი გამოწვევაა.

კიბერუსაფრთხოება სწრაფად განვითარებადი და მზარდი სფეროა, რომელიც ციფრული ტრანსფორმაციის ეპოქაში განსაკუთრებულ როლს თამაშობს გლობალური დღის წესრიგის ჩამოყალიბებაში, მსოფლიო ეკონომიკისა და საზოგადოების ფორმირებაში, ადმინისტრირებასა და მართვაში. პრაქტიკულად, აღარ არსებობს სოციალურ-ეკონომიკურ-საზოგადოებრივი საქმიანობის არცერთი დარგი, საჯარო თუ კერძო სექტორი, რომელიც დაცული იქნება კიბერსაფრთხეებთან მიმართებით.

კიბერსივრცე დანაშაულებრივი ქმედებების ჩასადენად საკმაოდ ხელსაყრელი გარემოა. ხშირ შემთხვევაში, ტექნოლოგიური ინოვაციები, დანაშაულის დისტანციურად და ფარულად ჩადენის შესაძლებლობა, მტკიცებულებათა ცვალებადობა, დამნაშავეთა იდენტიფიცირების სირთულეები და იურისდიქციასთან დაკავშირებული პრობლემები კრიმინალებისთვის ხელსაყრელი ფაქტორებია, რათა ინტერნეტსივრცე არაკანონიერი გზით გამოიყენონ. ძნელად მოიძებნება ეროვნული ან საერთაშორისო სტრატეგიული დოკუმენტები, საფრთხეების პოლიტიკის ანალიტიკური კვლევები, რომლებშიც კიბერსაფრთხეებისა და კიბერდანაშაულის გაზრდილ გამოწვევებსა და მნიშვნელოვნად მზარდ ტენდენციებზე არ იყოს ყურადღება გამახვილებული. გლობალურად ჩადენილი დანაშაულების 80-90% -ს კიბერდანაშაულის ელემენტები აქვს. „კიბერ“ ელემენტი თითქმის ყველა კატეგორიის დანაშაულის შემადგენელი ნაწილი ხდება. ინტერნეტსივრცე, ტექნოლოგიური გარემო, ერთი მხრივ, ხელს უწყობს სხვადასხვა დანაშაულებრივ ქმედებას (მაგ.: თაღლითობა, საკუთრების წინააღმდეგ მიმართული სხვა დანაშაულები, არჩევნების და წინასაარჩევნო კამპანიის დარღვევები და დანაშაულები; ნარკოტიკული საშუალებების რეალიზაცია ინტერნეტის გამოყენებით) და წარმოადგენს დანაშაულის ჩადენისთვის დამხმარე საშუალებას. მეორე მხრივ, ვიწრო, „კლასიკური გაგებით“, გვხვდება კომპიუტერული მონაცემებისა და სისტემების კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის წინააღმდეგ ჩადენილი დანაშაულები.

1კიბერუსაფრთხოება უზრუნველყოფს კიბერინციდენტების, ელექტრონული პროდუქტებისა და სერვისების დაცვას, რაც ზრდის მომხმარებელთა ნდობას და ელმმართველობის რეპუტაციას.

კიბერუსაფრთხოება თანაბრად მნიშვნელოვანი ხდება როგორც საერთაშორისო პოლიტიკის, ასევე ეროვნული უსაფრთხოების კონტექსტში, კრიმინოლოგიისა და სისხლის სამართლებრივი პოლიტიკის თვალსაზრისით, კორპორაციული პირებისა და ცალკე ინდივიდებისთვის. თანამედროვე ადამიანისთვის კი, მისი მოღვაწეობის ინტერესებისა თუ საქმიანობის სტილის მიუხედავად, ციფრულ სამყაროსთან ადაპტირება და შესაბამისი კიბერჩვევების გაუმჯობესება სასიცოცხლოდ აუცილებელ უნარს წარმოადგენს. კიბერინციდენტების რიცხვის ზრდის პარალელურად სულ უფრო მეტად მნიშვნელოვანი ხდება საზოგადოების წევრთა ცნობიერების ამაღლების საკითხი, კიბერკულტურის განვითარება და კიბერსივრცეში არსებულ საფრთხეებთან გამკლავების ეფექტიანი მექანიზმების დანერგვა. ეს ყოველივე, კიბერუსაფრთხო გარემოს მდგრადობას უზრუნველყოფს.

ადამიანური ფაქტორი მნიშვნელოვანი რისკია ციფრულ სამყაროში. როგორც საერთაშორისო კვლევები ადასტურებს, ყველაზე მეტი კიბერინციდენტი მსოფლიოში სწორედ ადამიანური რესურსის გამოყენებით ხორციელდება. მათ მიერ რისკებისა და საფრთხეების არასათანადო შეფასების, ცოდნისა და ცნობიერების სიმწირის ან/და განზრახ მიმართული არასანქცირებული ქმედებების შედეგად. დღესდღეობით ადამიანური შეცდომებით გამოწვეული კიბერინციდენტები მნიშვნელოვნად აღემატება კიბერშეტევათა რიცხვს. აღნიშნულის გათვალისწინებით, კიბერსივრცის უსაფრთხოება და დაცულობა მხოლოდ კიბერსაფრთხეებისა და რისკების შესახებ სამიზნე აუდიტორიის დროული ინფორმირებით მიიღწევა, მათ მიერ რისკების სათანადოდ გაცნობიერების, პრევენციული და სხვა სახის თავდაცვითი ღონისძიებების გატარების საშუალებით.

კიბერუსაფრთხოება, უპირველეს ყოვლისა, ყველა აქტორის ინდივიდუალური პასუხისმგებლობაა. თითოეული ვალდებულია იზრუნოს, მიიღოს ინფორმაცია საფრთხეებისა და რისკების შესახებ, შეისწავლოს და გამოიყენოს პრევენციისა და თავდაცვის წესები, რათა სათანადოდ გაუმკლავდნენ კიბერინციდენტებს მომხმარებლის დონეზე. სამართალდამცავ და კიბერუსაფრთხოებაზე უფლებამოსილ სტრუქტურებს კი მხოლოდ შესაბამისი აუცილებლობის შემთხვევაში მიმართონ.

შესაბამისად, მსოფლიოს მრავალი ქვეყანა, მათ შორის საქართველო, სტრატეგიულ მნიშვნელობას ანიჭებს ინფორმაციული საზოგადოების კიბერკულტურის, კიბერუსაფრთხოების საკითხებზე საზოგადოების ცნობიერების ამაღლებისა, მათი განათლებისა და გადამზადების საკითხებს. ამ პროცესში განსაკუთრებით მნიშვნელოვანია საჯარო სექტორში, როგორც ცენტრალურ, ასევე რეგიონებში დასაქმებული პირების კიბერშესაძლებლობების განვითარება ცნობიერების ამაღლების გზით, რადგან საჯარო სექტორში არსებული/დაცული მონაცემების კომპრომეტირებამ, საჯარო უწყებებზე მიმართულმა ინფორმაციულმა და კიბერშეტევამ შესაძლოა ქვეყნის უსაფრთხოებაზე, თავდაცვისუნარიანობასა და სოციალურ-ეკონომიკურ მდგომარეობაზე უმნიშვნელოვანესი გავლენა იქონიოს.

კიბერშესაძლებლობების განვითარებისკენ მიმართული ეს სახელმძღვანელო კიბერსივრცეში უსაფრთხოდ ოპერირებისთვის აუცილებელ ცოდნას სხვადასხვა მიმართულებით გადმოსცემს: კიბერუსაფრთხოების საფუძვლები, ინფორმაციული უსაფრთხოება და აქტივების მართვა, პერსონალური მონაცემების დაცვა კიბერსივრცეში, ინტერნეტი და მისი უსაფრთხოდ გამოყენება, ელექტრონული ფოსტის უსაფრთხოება, პერსონალური კომპიუტერის უსაფრთხოება, მობილური მოწყობილობის უსაფრთხოება, უკაბელო ქსელების უსაფრთხოდ სარგებლობა, პაროლების უსაფრთხოება და მართვა, სოციალური ქსელების უსაფრთხოდ სარგებლობა, ინფორმაციული წიგნიერება, არჩევნები და კიბერუსაფრთხოება, ინფორმაციული წიგნიერება, არჩევნები და კიბერუსაფრთხოება.

ტერმინთა განმარტება

კიბერსივრცე – სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის.

კიბერშეტევა – ქმედება, რომელიც იყენებს ელექტრონულ მოწყობილობას ან/და დაკავშირებულ ქსელს ან სისტემას კრიტიკული ინფრასტრუქტურის სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის/შეფერხების, განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით.

კიბერინციდენტი (კომპიუტერული ინციდენტი) – ინფორმაციული ან/და კიბერუსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.

კრიტიკული ინფრასტრუქტურა (კრიტიკული ინფრასტრუქტურის სისტემები) – სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის.

მალვეარი (Malware, malicious software) – მავნე კომპიუტერული პროგრამა (სხვადასხვა სახის ვირუსული პროგრამების საერთო სახელი), რომელიც ინფორმაციულ სისტემებზე არასანქცირებული შეღწევის, სენსიტიური ინფორმაციის შეგროვების, მოპარვის, განადგურების, შეცვლის, ან კომპიუტერზე უკანონო წვდომის მოსაპოვებლად გამოიყენება.

ფიშინგი (Phishing) – კიბერკრიმინალის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლის მოტყუებით შეძლოს კომპიუტერზე წვდომა. ფიშინგი, როგორც წესი, ხორციელდება ელ. ფოსტის საშუალებით, კომპიუტერის დაინფიცირება კი მოცემულ ბმულზე ღილაკის დაჭერით ხდება ან თანდართული ფაილის ჩამოტვირთვით. ფიშინგის განსაკუთრებულ ფორმას წარმოადგენს ე.წ. Spear-Phishing, რომელიც განკუთვნილია მომხმარებლის ვიწრო და სპეციფიური წრისათვის (გარკვეული ცოდნის, ინფორმაციის მატარებელი ინდივიდი ან ჯგუფი). ე.წ. Spear-Phishing-ი საჭიროებს კარგად მომზადებულ კონტექსტს ნდობის მოსაპოვებლად. ფიშინგშეტყობინების/ელ.ფოსტის დაგზავნა ხდება ერთობლივად ბევრ მისამართზე, ხოლო ე.წ. Spear-Phishing-ის გაგზავნა მიზანმიმართულად, ცალკეული ინდივიდების ელ. მისამართებზე.

ვებგვერდის სერვისის უარყოფა (Denial-of-service/DoS attack) – კიბერთავდასხმის ერთ-ერთი სახე, სადაც თავდამსხმელი ცდილობს გახადოს ინტერნეტრესურსი ხელმიუწვდომელი.

სერვისის დისტრიბუციული/განაწილებული უარყოფა Distributed Denial-of-Service (DDoS) attack – არის მასშტაბური DoS შეტევა, სადაც თავდამსხმელი იყენებს ერთ ან მეტ, ხშირ შემთხვევაში, ათასობით IP მისამართს. ამ ტიპის შეტევები ძირითადად ხდება ვებგვერდებზე.

დიფეისი/Defacement – დაბალტექნოლოგიური კიბერშეტევის ფორმა, რომელიც არასანქცირებულად ცვლის ვებგვერდის გარეგნულ იერსახეს, ხშირად პირველ გვერდს. ძირითადად, გამოიყენება კიბერტერორისტების მიერ საპროტესტო მესიჯის, პროპაგანდისტული მასალის ან სხვა კონტენტის გასავრცელებლად.

დარქნეტი/Darknet – ინტერნეტქსელი შეზღუდული წვდომით, რომელიც უმთავრესად არალეგალური მიზნებისთვის გამოიყენება, მათ შორის უკანონო საქონლისა და მომსახურების გაცვლისთვის – ე.წ. შავი ინტერნეტბაზარი.

განვითარების ძლიერი საფრთხე/Advanced Persistent Threat (APT) – მიზანმიმართული განვითარებული საფრთხეები, მაღალტექნოლოგიური და ხანგრძლივმოქმედი კიბერშეტევა, რომლის დროსაც შემტევი მხარე აღწევს სამიზნის ინფორმაციულ სისტემაში და ხანგრძლივი დროის მანძილზე შეუმჩნევლად აგროვებს ინფორმაციას. როგორც წესი, სახელმწიფო აქტორები იყენებენ APT-ს.

რენსომვეარი (Ransomware) – მავნე პროგრამა, რომელიც კომპიუტერულ სისტემაში შიფრავს ფაილებს, დოკუმენტებს, „მძევლად ჰყავს აყვანილი" მომხმარებლისთვის მნიშვნელოვანი ინფორმაცია და მისი გაშიფრული ფორმით დაბრუნების სანაცვლოდ მომხმარებელს სთხოვს გამოსასყიდს. ხშირად, რენსომვეარს ყალბი ანტივირუსის ფორმაც აქვს და პოპ-აპის სახით ამოხტება ხოლმე ეკრანზე და მომხმარებელს კომპიუტერულ უსაფრთხოებას სთავაზობს.

ინფორმაციული უსაფრთხოება – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას.

ინფორმაციული აქტივი – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის.

ტროლინგი (Trolling) – საზოგადო ტერმინი ყველა ისეთი ქმედების გამოსახატავად, რომელიც მიმართულია ინტერნეტსივრცეში (ძირითადად სოციალურ მედიაში, პოპულარულ ფორუმებზე) კონკრეტული ინდივიდის ან ინდივიდთა ჯგუფების მიმართ დამამცირებელი, შეურაცხმყოფელი, შემავიწროვებელი, ცილისმწამებლური შინაარსის ინფორმაციის გავრცელებისკენ.

პერსონალური მონაცემების, ვინაობის მითვისება, მოპარვა (Identity theft) – ერთი პირის მიერ მეორე სუბიექტის ინფორმაციის, მონაცემების ან დოკუმენტების მოპოვება და თავის საკუთრებად წარმოჩენა, ამ პირის სახელით საქონლის თუ მომსახურების მისაღებად.

მზა ჩანაწერი (Cookies) – კომპიუტერული პროგრამა, რომელიც მონიტორინგს უწევს და ასახავს კომპიუტერის მომხმარებლის აქტივობას. „მზა ჩანაწერი" წარმოადგენს მცირე ზომის ტექსტურ ფაილს, რომელსაც ვებგვერდი ინახავს მომხმარებლის კომპიუტერში ან მობილურ ტელეფონზე, როდესაც მომხმარებელი საიტს სტუმრობს. ეს ჩანაწერი საშუალებას აძლევს ვებგვერდს დაიმახსოვროს მომხმარებლის ქმედებები და პრეფერენციები.

უკანა კარი (Backdoor) – ავტორიზაციისთვის დადგენილი მოთხოვნების გვერდის ავლით კომპიუტერის სისტემაზე დისტანციურად წვდომის მიღება. ეს არის ჯაშუშური მალვეარი, რომელიც გამოიყენება არა მხოლოდ ინფორმაციის მიტაცებისთვის, არამედ კომპიუტერის უკანონოდ სამართავადაც, კომპიუტერული უსაფრთხოების მექანიზმების გვერდის ავლით.

პორტატული მედია საშუალებები – ინფორმაციის მატარებელი მოწყობილობები (კომპაქტდისკები CD, USB მეხსიერების ბარათები).

ტროიანი (Trojan Horse) – მალვეარი, რომლის მიზანია ინფორმაციულ აქტივებზე წვდომა ან/და კომპიუტერული სისტემების დაზიანება. ტროიანი თავს აჩვენებს მომხმარებელს თითქოს იგი არის სრულიად სანდო და უვნებელი, სთავაზობს ბენეფიტებს, რათა მსხვერპლს მოტყუებით დააინსტალირებინოს თავი კომპიუტერულ სისტემაში და ამგვარად მოიპოვოს წვდომა სასურველ სისტემაზე.

ვირტუალური კერძო ქსელი (VPN) – არის ქსელი, რომელიც აგებულია საზოგადოებრივ ქსელში, როგორიცაა ინტერნეტი, კერძო ქსელთან დასაკავშირებლად, მაგალითად კომპანიის შიდა ქსელი. VPN გადაწყვეტილებები უზრუნველყოფს უსაფრთხო და დაშიფრულ კომუნიკაციას საჯარო ინტერნეტქსელში, რათა დაცული იქნეს მნიშვნელოვანი ინფორმაცია არაავტორიზებული წვდომისგან, ჰაკერებისგან. VPN საშუალებას აძლევს მომხმარებლის კომპიუტერს გააგზავნოს და მიიღოს მონაცემები გაზიარებულ ან საჯარო ქსელებს შორის, ისე თითქოს ისინი კერძო ქსელების ნაწილი იყოს, მათ შორის, დაცულია კერძო ქსელის ფუნქციონირების, უსაფრთხოების და მართვის პოლიტიკა. ეს ხდება ვირტუა-

ლური წერტილიდან წერტილამდე კავშირის დამყარებით, სპეციალური კავშირების გამოყენებით, დაშიფვრით ან ამ ორი მექანიზმის კომბინაციით. იგი არ არის ადვილი დასაყენებელი და, როგორც წესი, ისინი საბოლოო მომხმარებლებისთვის მიუწვდომელია. ძირითადად ორგანიზაციები უზრუნველყოფენ თანამშრომლებს VPN კავშირით.

სნიფინგ (Sniffing) – ქსელური პაკეტების სნიფინგი არის ქსელში გადაცემულ მონაცემთა პაკეტების მოსმენა და აღება, მათზე არასანქცირებული წვდომის მოპოვება.

ტორენტ გვერდები – ფაილების (აუდიო-ვიდეო მასალის) გადმოწერა-გაზიარების მიზნით შექმნილი სისტემა, რომელთან დაკავშირებითაც ხშირ შემთხვევაში დგება საავტორო უფლებებთან დაკავშირებული სამართლებრივი პრობლემები და მიმოცვლილი ფაილებით მავნე პროგრამული უზრუნველყოფისა და ვირუსების გავრცელების შემთხვევები.

ბოტნეტი – ბოტნეტი არის ინტერნეტ ქსელში ჩართული კომპიუტერების ერთობლიობა, რომლებსაც დაკარგული აქვთ დამოუკიდებლად ოპერირებისა და თავდაცვის უნარი, მათი დისტანციური მართვა მესამე პირის მიერ ხორციელდება. ბოტნეტი ფართოდ გამოიყენება DDoS კიბერ შეტევებისთვის: ზომბირებული კომპიუტერებიდან ერთდროულად იგზავნება ათასობით მოთხოვნა სამიზნე სერვერზე (ვებ-გვერდზე), შედეგად სერვერი ვერ ასწრებს დიდი მოთხოვნის დამუშავებას და ხდება ხელმიუწვდომელი. ბოტნეტი მრავალი კიბერშეტევისთვის გამოიყენება, მათ შორის სპამის მეშვეობით ვირუსის/მალვეარის გავრცელებით, დამთავრებული სახელმწიფო ქსელებზე კიბერშეტევებით.

ბოტი – იგივე რობოტი, ეს არის ავტომატიზირებული ანგარიში სოციალურ მედიაში, რომელიც ადამიანის ჩარევის გარეშე მოქმედებს. იგი გამოიყენება კონკრეტული ინფორმაციის, სტატიის, პოსტის ხელოვნურად პოპულარულად წარმოსაჩენად (ბევრი მომხმარებელი, სინამდვილეში კი ბოტის მოწონებით). ბოტები ხშირად გამოიყენება პოლიტიკური განცხადებებისთვის დიდი მნიშვნელობის მისაცემად.

ტროლი – ბოტებისგან განსხვავებით, ტროლების ონლაინ მედია ანგარიშების უკან რეალური პირი/პირებია, რომლებიც სხვადასხვა მიზნით (მაგ.: ფინანსური დაინტერესება, ჯაშუშობა) მიზანმიმართულად ქმნიან ბლოგებს, წერენ სტატუსებს, კომენტარებს პოლიტიკურ მოვლენებზე გავლენის მოსახდენად, ჯანსაღი დისკუსიისთვის ხელის შესაშლელად, კონკრეტული პირების დისკრედიტაციისთვის, საზოგადოებრივი აზრის პოლარიზაციისთვის. ტროლები ორგანიზებულად ახორციელებენ კოორდინირებულ არაავთენტურ ქცევას.

ელფოსტის სპუფინგი/mail spoofing – წარმოადგენს კიბერსივრცეში თაღლითობის ფორმას, რომლის დროსაც გამგზავნი პირის ელექტრონული ფოსტის მისამართი გაყალბებულია – ხშირად მიმსგავსებულია სანდო წყაროს და ადრესატს უქმნის საფუძვლიან ნდობას, რომ წერილი მიღებული აქვს სანდო/მისთვის ცნობილი წყაროდან, რის გამოც უზიარებს გამომგზავნს მოთხოვნილ პერსონალურ ინფორმაციას ან/და წვდომას აძლევს თავის ინფორმაციულ სისტემებზე.

მოდული 1

შესავალი – კიბერუსაფრთხოების სიტუაციური ანალიზი

საქართველო მსოფლიოში ერთ-ერთი პირველი ქვეყანაა, რომელსაც სახმელეთო, საჰაერო და საზღვაო სივრცის დაცვასთან ერთად, ჯერ კიდევ 2008 წელს, რუსეთ-საქართველოს ომის დროს, კრემლის მხრიდან წარმოებული კიბერსაომარი მოქმედებებისგან საკუთარი კიბერსივრცის უსაფრთხოების უზრუნველყოფა გამოწვევად ექცა. იმ პერიოდში საქართველოს როგორც საჯარო, ასევე კერძო სექტორი არ იყო მზად კიბერშეტევებთან გასამკლავებლად. ქვეყანაში არარსებობდა კიბერშესაძლებლობებით და შესაბამისი უფლებამოსილებით აღჭურვილი სამთავრობო უწყებები, შესაბამისად საქართველომ შეტევასთან გასამკლავებლად და შედეგების აღმოსაფხვრელად მყისიერი დახმარება ნატოსა და ევროკავშირის პარტნიორი ქვეყნების კიბერსპეციალისტებისგან მიიღო. სწორედ ეს მოვლენა გახდა საქართველოში კიბერუსაფრთხოების ინსტიტუციური, სტრატეგიული, სამართლებრივი, ტექნიკური და თანამშრომლობითი ეკოსისტემის საფუძვლების ჩამოყალიბების წინაპირობა.

ბოლო ათი წლის განმავლობაში საქართველომ მიიღო და განახორციელა კიბერუსაფრთხოების ორი თანმდევი ეროვნული სტრატეგია შესაბამისი სამოქმედო გეგმით; ჩამოყალიბდა ინფორმაციული და კიბერუსაფრთხოების სამართლებრივი ბაზა – „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და მისგან გამომდინარე კანონქვემდებარე აქტები; საქართველო შეუერთდა კიბერდანაშაულის შესახებ ბუდაპეშტის კონვენციას; განისაზღვრა კრიტიკული ინფორმაციული სისტემის სუბიექტები და კიბერუსაფრთხოების უზრუნველყოფაზე პასუხისმგებელი სახელმწიფო ორგანოები; საფუძველი ჩაეყარა ქვეყნის შიგნით საჯარო-კერძო პარტნიორობას კიბერუსაფრთხოების ფორუმის სახით; საქართველოს სამთავრობო უწყებების ორგანიზებით განხორციელდა ცნობიერების ამაღლების კამპანიები, სამიზნე ჯგუფების გადამზადება. აღსანიშნავია, რომ საქართველოს საგარეო და უსაფრთხოების პოლიტიკის სტრატეგიულ მიზანს ევროკავშირსა და ნატოში გაწევრიანება წარმოადგენს, რაც სრულად ასახავს ქვეყნის მოსახლეობის ურყევ ნებას. შესაბამისად, საქართველო თანამშრომლობს კიბერთავდაცვისა და უსაფრთხოების მიმართულებით ევროკავშირისა და ნატოს წევრ სახელმწიფოებთან, მონაწილეობს როგორც ინდივიდუალურად, ისე მათი ეგიდით გამართულ სხვადასხვა სახის პროექტში, სტრატეგიულ თუ ტექნიკურ სწავლებებში, კიბერუსაფრთხოების საერთაშორისო პროექტებსა და შეხვედრებში (EU, NATO, OSCE, UN, EaP, CoE, EUROPOL & INTERPOL, CEPOL, ENISA).

საქართველოს მიერ კიბერუსაფრთხოების უზრუნველყოფისკენ გადადგმული ნაბიჯები, განხორციელებული რეფორმები ბოლო ათწლეულების მანძილზე პოზიტიურად იყო შეფასებული საერთაშორისო რეიტინგებსა და ინდექსებში. აღმოსავლეთ პარტნიორობისა და პოსტსაბჭოთა ქვეყნებს შორის კიბერუსაფრთხოების განვითარების თვალსაზრისით, საქართველო მოწინავე პოზიციებზე იმყოფებოდა და საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) კიბერუსაფრთხოების გლობალური ინდექსის (GCI – Global Cybersecurity Index) მაჩვენებლებით – მსოფლიოში 2017 წელს მე-8 ადგილით ითვლებოდა სამხრეთ კავკასიისა და შავი ზღვის აუზის ქვეყნებს შორის რეგიონის ლიდერ ქვეყნად. საქართველო წინ უსწრებდა აღმოსავლეთ და ცენტრალური ევროპის არაერთ სახელმწიფოს კიბერსფეროს განვითარებით, თუმცა 2018 წლიდან საქართველომ დაკარგა წარმატებული ქვეყნის პოზიციები და რეგიონის ლიდერიდან 2018 წელს მე-18 ადგილზე გადაინაცვლა, ხოლო 2021-ში უკვე მსოფლიოს ქვეყნებს შორის 55-ე ადგილს დასჯერდა. საქართველოს კიბერგარემოს მდგომარეობის რადიკალური გაუარესების მიზეზად, ერთი მხრივ, შესაძლოა მივიჩნიოთ სხვა ქვეყნების კიბერუსაფრთხოების სისტემის სწრაფი და წარმატებული განვითარება, ხოლო, მეორე მხრივ, საქართველოს მიერ სტრატეგიული რეფორმების დაყოვნება და კიბერუსაფრთხ-

ოების საკითხების მიმართ სახელმწიფოებრივი ხედვის არარსებობა.

მიუხედავად გარკვეული აღმავლობისა, კიბერსაფრთხეებსა და რისკებთან გამკლავების მიმართულებით საქართველოს ჯერ კიდევ დიდი ძალისხმევა სჭირდება.

საქართველოს სისხლის სამართლის კოდექსით დასჯადია კიბერდანაშაულის შემდეგი სახეები:

• კომპიუტერულ სისტემაში უნებართვო შეღწევა (მუხლი 284)[2];

• კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება (მუხლი 285) – კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა, მსგავსი მონაცემის უნებართვო დამზადება, შეძენა, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა;

• კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა (მუხლი 286) – კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია;

• კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით (მუხლი 286 პრიმა) – თავისთვის ან სხვისთვის ქონებრივი უფლების მოპოვების ან ნებისმიერი სახის ფინანსური სარგებლის მიღების მიზნით კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის უნებართვო ჩასმა, წაშლა, შეცვლა ან დაფარვა ან კომპიუტერული სისტემის ფუნქციონირებაში ნებისმიერი სახის უნებართვო ჩარევა, რამაც სხვისთვის ფინანსური ზიანის მიყენება გამოიწვია;

• ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა (მუხლი 286 სეკუნდა) – კომპიუტერული მონაცემის უნებართვო ჩასმით, წაშლით, შეცვლით ან დაფარვით ყალბი ოფიციალური კომპიუტერული მონაცემის მიღება მისი ნამდვილ/უტყუარ მონაცემად გასაღების ან/და გამოყენების მიზნით, გასაღება ან/და გამოყენება.

კომპიუტერულ ინციდენტებზე დახმარების ეროვნული და სამთავრობო ჯგუფის (CERT.GOV.GE) მიერ ინციდენტების აღმოჩენისა და მათზე რეაგირების სხვადასხვა ტექნოლოგიური საშუალების გამოყენებით (ქსელისა და IP მონიტორინგის სისტემა, პორტალები, სენსორები და ა.შ.) მიღებული სტატისტიკა ცხადყოფს, რომ 2014 წლიდან 2019 წლამდე დარეგისტრირებული ინციდენტების რაოდენობა, სულ მცირე, ორჯერ გაიზარდა. ამასთან, იმატა დაინფიცირებული IP მისამართების რიცხვმა და პორტალებთან დაკავშირებულმა უსაფრთხოების მოვლენებმა.

საქართველოს გეოპოლიტიკური მდებარეობა, ქვეყნის პოლიტიკური კურსი და ევროატლანტიკურ სტრუქტურებში ინტეგრაციისკენ სწრაფვა, საქართველოს, პირველ რიგში, რუსეთის ფედერაციის მხრიდან ხდის პოლიტიკურად მოტივირებული კიბერშეტევების, ინფორმაციული პროპაგანდის, ცრუინფორმაციის, კიბერჯაშუშობისა და კიბერტერორიზმის სამიზნედ (მაგ.: Georbot-ის საქმე, APT28, 2019 წლის ოქტომბრის ფართომასშტაბიანი თავდასხმა, 2020 წლის სექტემბერში რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის მონაცემთა ბაზებზე კიბერთავდასხმა).

შინაგან საქმეთა სამინისტროს სტატისტიკაზე დაყრდნობით, ყოველწლიურად მატულობს კიბერდანაშაულის რიცხვი. თუკი 2017 წელს რეგისტრირებული კიბერდანაშაულის მაჩვენებელი არ სცდებოდა 500 მაჩვენებელს, 2020 წელს ამ ნიშნულმა 2000-ს გადააჭარბა. 2020 წელს რეგისტრირებული კიბერდანაშაულების რიცხვი 20%-ით იმ დროს გაიზარდა, როდესაც კონვენციური დანაშაულების რიცხვმა ქვეყანაში იკლო. დღესდღეობით ფართოდ არის გავრცელებული კიბერდანაშაულის ისეთი სახეები, როგორიცაა: კომპიუტერულ სისტემაზე უნებართვო წვდომა, კომპიუტერულ მონაცემთა არამართლზომიერი დაუფლება, მონაცემთა ხელყოფა, კომპიუტერული

2 ამავე მუხლის მიხედვით, კომპიუტერული სისტემა არის ნებისმიერი მოწყობილობა/მექანიზმი ან ერთმანეთთან დაკავშირებულ მოწყობილობათა/მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, მობილური ტელეფონი). კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას. ხოლო უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისათვის.
კანონის ბმული:

მოწყობილობების არასანქცირებული გამოყენება, არასრულწლოვანთა პორნოგრაფიასა და ინტელექტუალურ საკუთრებასთან დაკავშირებული დანაშაულები. განსაკუთრებით ფართოდ გავრცელებული შემთხვევებია კიბერომი, საინფორმაციო ომი, კიბერჯაშუშობა, სახელმწიფო აქტორების მიერ მართული კიბერშეტევები, კიბერდანაშაული და კიბერმეთოდებით ჩადენილი დანაშაულები, ტრანსსასაზღვრო ორგანიზებული დანაშაულები. ბოლო პერიოდში კრიტიკული ინფრასტრუქტურების წინააღმდეგ მიმართულ შეტევებს შორის ყველაზე გავრცელებულია „ფიშინგი“ (phishing), „რანსომვეარი“ (Ransomeware), „დიფეისი“ (deface), „დიდოსი“ (DS) და „ელფოსტის სპუფინგი“ (mail spoofing).

რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ წარმოებული ინფორმაციული ომი, პროპაგანდისა და დეზინფორმაციის მაღალი მაჩვენებლით ხასიათდება. ეს პროცესი ხელსაყრელ ნიადაგს ქმნის საზოგადოებრივი აზრის მანიპულაციისთვის, რაც, მიმდინარე სამხედრო ოკუპაციის კვალდაკვალ, ეროვნული უსაფრთხოებისთვის სასიცოცხლო მნიშვნელობის საფრთხეს წარმოადგენს.

საქართველოს მოსახლეობის არჩევანზე, რომელიც ეროვნული უსაფრთხოების მდგრადობის გაძლიერებას, რუსული გავლენისგან გათავისუფლებასა და დასავლურ სტრუქტურებში ინტეგრაციას ითვალისწინებს, ხდება მასობრივი და მიზანმიმართული ზემოქმედება, სახელმწიფოს საგარეო პოლიტიკური კურსის სახეცვლილებისა და ერთგვარად ნეიტრალური საგარეო კურსის გატარების მიზნით.

ევროინტეგრაციის პროცესში მიღწეული წარმატებისა და ამ პროცესით გამოწვეული განვითარების გადაფარვა, საქართველოში დასავლური გზის მარგინალიზება და დასავლელი პარტნიორების წინაშე საქართველოს როლის დაკნინება რუსეთის ფედერაციის ის სტრატეგიული მიზანია, რომელსაც პრაქტიკულ დონეზე მათ მიერვე გამოყენებული ყველა მეთოდი – კინეტიკური, ჰიბრიდული თუ ინფორმაციული ომი – მკაცრად ემსახურება.

ხაზგასასმელია ის გარემოებაც, რომ იზრდება რუსეთის ფედერაციის მხრიდან მომდინარე საფრთხეები (Advanced Persistent Threat), რომელთა მიზანია საქართველოს კერძო და საჯარო კრიტიკული ინფრასტრუქტურების ინფორმაციასთან არაავტორიზებული წვდომა.

ტერორისტების მიერ ინტერნეტის გამოყენება კომპიუტერული საშუალებებით ჩადენილი დანაშაულის კიდევ ერთი სახეობაა. ტერორისტები სულ უფრო ხშირად მიმართავენ ინფორმაციულ სისტემებს ინფორმაციის გავრცელების, კომუნიკაციისა და პროპაგანდის მიზნით. უკანასკნელი წლების პრაქტიკამ დაადასტურა, რომ ტერორისტული ორგანიზაციები, მაგალითად, ისლამური სახელმწიფო ინტენსიურად იყენებს თანამედროვე ინფორმაციულსა და საკომუნიკაციო საშუალებებს, როგორც ტერორისტულ ორგანიზაციაში რეკრუტირებისა და ტერორისტული პროპაგანდის გავრცელებისთვის, ისე ქვეყნის შიგნით ტერორისტული ქსელის შესაქმნელად. მისი განეიტრალება შესაძლებელი გახდა 2017 წლის ნოემბერში ჩატარებული ფართომასშტაბიანი კონტრტერორისტული ოპერაციის საშუალებით.

გარდა ზემოაღნიშნული მაღალი ინტენსივობისა, სახელმწიფო აქტორების ჩართულობით მართული მიზანმიმართული შეტევებისა, მნიშვნელოვან სამიზნედ იქცა კრიტიკული ინფორმაციული ინფრასტრუქტურა; კერძოდ, სახელმწიფოსა და საზოგადოებისთვის კრიტიკულად მნიშვნელოვანი ფუნქციების განხორციელებისა და სერვისების მიწოდების პროცესში გამოყენებული ინფორმაციული სისტემები და ტექნოლოგიები.

ბოლო პერიოდის პრაქტიკა აჩვენებს, რომ სახელმწიფო კრიტიკულ სექტორებთან ერთად შეტევის სამიზნედ სულ უფრო ხშირად გვევლინებიან კომერციული სუბიექტებიც, რაც მიზნად ისახავს აღნიშნული სექტორისთვის, სულ მცირე, რეპუტაციული ზიანის მიყენებას, სათანადო პირობების არსებობისას, მის პარალიზებას. ზემოთქმულის მაგალითია 2016 წელს საქართველოში, საბანკო სექტორისა და სახელმწიფო ელექტრონული ფინანსური სერვისების წინააღმდეგ განხორციელებული ფართომასშტაბიანი „DDoS“ შეტევა, რომლის შედეგადაც მცირე ხნით, თუმცა, მაინც შეფერხდა ონლაინ საბანკო სერვისებისა და სახელმწიფო საგადასახადო სისტემის მუშაობა.

გარდა ამისა, ფიზიკური პირები, იურიდიული პირებისა და სახელმწიფო ორგანოების კვალდაკვალ, ძალიან ხშირ შემთხვევაში ხდებიან ფინანსურად თუ სხვაგვარად მოტივირებული კიბერშეტევების სამიზნე ობიექტები. როგორც აღმოჩნდა, ინდივიდი უფრო ხშირად ხდება კიბერდანაშაულის მსხვერპლი/სამიზნე, ვიდრე კლასიკური დანაშულისა.

ვიქტიმიზაციის კვლევები კიბერდანაშაულისა და კონვენციული დანაშაულის შედარების საფუძველს წარმოადგენს. გაეროს კვლევის მიხედვით[3], მსოფლიოს მასშტაბით სხვადასხვა ქვეყნის 1-დან 17 პროცენტამდე ინტერნეტმომხმარებელი ონლაინ საკრედიტო ბარათებთან დაკავშირებული თაღლითობის, პერსონალური მონაცემების ქურდობის, ფიშინგის/ფიშინგის მცდელობის და ელფოსტის ანგარიშზე უნებართვო წვდომის მსხვერპლი გახდა. შედარებისთვის, ამავე ქვეყნებში ჩვეულებრივი ქურდობის, ყაჩაღობისა და მანქანის ქურდობის 5 პროცენტით ნაკლები მაჩვენებელი აღინიშნება. ეს ყოველივე ცხადყოფს, რომ კიბერდანაშაულის მსხვერპლთა მაჩვენებლები კლასიკურ დანაშაულთან შედარებით გაცილებით მაღალია. განვითარებად ქვეყნებში, როგორიც საქართველოა, კიბერდანაშაულის მსხვერპლთა მაღალი მაჩვენებელი, უპირველეს ყოვლისა, განპირობებულია პრევენციული მექანიზმების, მათ შორის კიბერგანათლებისა და ცნობიერების არარსებობით.

შესაძლოა, კიბერინციდენტებისა და კომპიუტერული საფრთხეების ზრდამ სასიცოცხლოდ მნიშვნელოვანი, ინფორმაციული სისტემებისა და კრიტიკული სერვისების ფუნქციონირების შეწყვეტა ან შეჩერება გამოიწვიოს. ეკონომიკური აქტივობების შეზღუდვა, მნიშვნელოვანი ფინანსური ზარალი, ინდივიდების ფინანსური, რეპუტაციული ზარალი, პირადი ცხოვრების ხელშეუხებლობასა და ციფრულ სამყაროში მომხმარებლების ყოველდღიური საქმიანობისათვის ხელის შეშლა, იწვევს მომხმარებელთა ნდობის დაკარგვას და ჯამში ელექტრონულ მმართველობაზე ნეგატიურად აისახება. დღეს საქართველოს სახელმწიფო და კერძო სექტორში არსებული კრიტიკული ინფრასტრუქტურები ყოველდღიურ საქმიანობაში, უმეტესწილად, ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებს იყენებენ. შესაბამისად, მათ მიერ გამოყენებული ტექნოლოგიების კომპრომეტირება, ამით სახელმწიფო და ბიზნესინტერესებისა თუ ინდივიდუალური მომხმარებლების დაზარალება მრავალი დანაშაულებრივი დაჯგუფების მიზანია. კიბერდანაშაულის მიერ დამდგარი ზიანი გაცილებით მაღალია, ვიდრე ეს 2008 წელს იყო, სწორედ სახელმწიფო და კერძო სერვისების ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე მაღალი დამოკიდებულების გამო.

–იხ. ცხრილი: კიბერშეტევებით გამოწვეული პოტენციური ზიანი, ზარალი

კიბერდანაშაული ჯერ კიდევ „მომავლის“ დანაშაულს წარმოადგენს საქართველოსთვის. კიბერსაფრთხეები მუდმივად განვითარებადი ფენომენია, ინტერნეტ მომხმარებლების ონლაინ ქცევაზე დაკვირვებითა და არსებული გარემო პირობების, მიმდინარე ტენდენციების შესწავლით კიბერკრიმინალები შეტევის ახალ ვექტორებს იკვლევენ, ტექნოლოგიურად უფრო დახვეწილ და რთულ კიბერსაფრთხეებს ქმნიან. კოვიდ პანდემიაც, როგორც გლობალური გამოწვევა, არ ყოფილა ამ მხრივ გამონაკლისი და კიბერსივრცის ბნელმა სამყარომ ჯანდაცვის საერთაშორი-

3 კიბერდანაშაული (კვლევის ანგარიში), UNOCD იხილეთ ბმული:

ოპერაციული სისტემის გაჩერება	ბიზნესპროცესების გაჩერება	მონაცემების დაკარგვა	ფინანსური თაღლითობა	სამართლებრივი დაცვა
ინციდენტზე რეაგირების ხარჯები	ინტელექტუალური საკუთრების მისაკუთრება	კიბერ-გამოძალვა რენსომი	ფიზიკური აქტივების დაზიანება	სისტემების ფიზიკური დაზიანება
პირადი ცხოვრების დარღვევა-კომპენსირება	ქსელის უსაფრთხოების დარღვევა-პასუხისმგებლობა	რეპუტაციული ზიანი	მარეგულირებელ მოთხოვნებთან შესაბამისობა	პროფესიული სერვისები
ჯარიმები და პასუხისმგებლობები	კომუნიკაცია და მედია	ტექნოლოგიური შეცდომები	გარემოსა და ბუნებრივი პირობების დაზიანება	.....

სო კრიზისით ბოროტად სარგებლობა გადაწყვიტა. საქართველოში არ ჩატარებულა საფუძვლიანი კვლევა იმის შესახებ, თუ როგორ იმოქმედა პანდემიამ კიბერშეტევებისა და კიბერდანაშაულის სტატისტიკურ მაჩვენებლებზე, ან რამდენად შეიცვალა საფრთხის სამიზნეები თუ აქტორები. იმის გათვალისწინებით, რომ საქართველოს კიბერსივრცის გამოწვევები მეტწილად იმეორებს საერთაშორისო მასშტაბით არსებულ ტენდენციებს, შეგვიძლია ვივარაუდოთ, რომ ინტერპოლის მიერ კოვიდ პანდემიით გამოწვეული კიბერსაფრთხეები[4] შესაბამისად რელევანტური და აქტუალურია ჩვენთან დაკავშირებით. კერძოდ:

– პანდემიის პირობებში, როდესაც მთელი სამყარო გადავიდა ონლაინ ცხოვრების რეჟიმში და ტექნოლოგიებსა და ინტერნეტზე დამოკიდებულებამ არნახულ მაჩვენებელს მიაღწია, გაიზარდა კოვიდ პანდემიის თემატიკის საფარქვეშ ფიშინგული შეტევები, კომპიუტერულ სისტემებში უნებართვო შეღწევა და პერსონალური ინფორმაციის მოპარვა. „კორონა“, „კოვიდი“ საკვანძო სახელების გამოყენებით რეგისტრირებული იქნა მრავალი ახალი ვებგვერდი (პალო ალტოს ქსელის – Palo Alto Networks მონაცემებით 2020 წლის მარტის ბოლოსთვის 2,022 მავნე და 40,261 მაღალი რისკის შემცველი ახალი დომენური სახელები იქნა გამოვლენილი), რომლებიც ინფორმაციის მიღების სურვილით ვებგვერდზე შემოსული მომხმარებლების კომპიუტერულ სისტემებში მავნე კოდის ინსტალაციითა და ვირუსების გავრცელებით მოქმედებდა.

– კოვიდ პანდემიასთან დაკავშირებული დეზინფორმაცია და ყალბი სიახლეები საკმაოდ აქტუალური ფენომენი გახდა, როგორც საქართველოში, ასევე საერთაშორისო მასშტაბით. სწორედ ამიტომაც საერთაშორისო სამართალდამცავი ორგანიზაციების, მათ შორის, ინტერპოლის შეფასებით ინფორმაციული საფრთხეები განიხილება კიბერდანაშაულის კონტექსტში, როგორც სისხლის სამართლებრივი სისტემის გამოწვევა. პანდემიის თემატიკაზე დეზინფორმაცია ან ყალბი ახალი ამბები, ისევე როგორც ანტივაქსერული მიმართვები ძირითადად ვრცელდებატროლების და ყალბი ონლაინ მომხმარებლების ანგარიშებით პანიკისა და დესტაბილიზაციის გამოწვევის, მთავრობების ან მათი ჯანდაცვის ორგანოების მიმართ უნდობლობის დათესვის მიზნით.

– რენსომვეარი და DDoS შეტევები კოვიდ პანდემიის ბრძალაში ჩართული სუბიექტების, ძირითადად სამთავრობო, სამედიცინო, სამეცნიერო ობიექტების წინააღმდეგ გამოსასყიდის მისაღებად ან მათი გათიშვით მდგომარეობის მართვის, ტესტირებისა და მკურნალობის პროცესის შეფერხების მიზნით.

– დისტანციურად მომუშავე თანამშრომლობის წინააღმდეგ განხორციელებული შეტევებით (მავნე პროგრამული უზრუნველყოფა, ბიზნეს ელ-ფოსტაზე შეტევა და აშ) კორპორატიულ ინფორმაციულ სისტემებზე, კრიტიკულ ინფორმაციულ სისტემებზე წვდომის მოპოვება და კორპორატიული მონაცემების დაუფლება ან/და მათი ინფრასტრუქტურის მწყობრიდან გამოყვანა.

მომავალ ხუთწლიან პერსპექტივაში საქართველოში კიბერსაფრთხეებისა და კიბერდანაშაულის რიცხვი სწრაფად მზარდ ტენდენციას შეინარჩუნებს. დიდი ალბათობით კიბერდანაშაული 2020 წლის მაჩვენებელთან შედარებით წელიწადში საშუალოდ 25-30%-ით გაიზრდება და 2022 წელს შსს-ს მიერ რეგისტრირებულ სისხლის სამართლის საქმეებში კიბერდანაშაულის წილი 5%-ს გადააჭარბებს[5]. რა იძლევა ექსპერტთა მიერ გამოთქმული ამგვარი ვარაუდის საფუძველს? ყოველწლიურად იზრდება ქართული საზოგადოების დამოკიდებულება ინტერნეტრესურსებსა და ტექნოლოგიებზე ,,სა-ჯარო და კერძო სერვისების გაციფრულება. ქვეყნის სოციალურ-ეკონომიკური განვითარება, გეოპოლიტიკური კურსი და საგარეო ურთიერთობების კონტექსტი იმ პირობებში, როდესაც არ გვაქვს პრევენციული და პროაქტიული მექანიზმები, ცნობიერებისა და კიბერგანათლების საბაზისო უნარ-ჩვევები, იძლევა კიბერდანაშაულისა და კიბერსაფრთხეების ზრდის პროგნოზირების წინაპირობას. სამწუხაროდ, ამ საგარეო და შიდა კომპლექსურ დეტერმინანტებზე საქართველოს მოკლევადიან პერსპექტივაში არ გააჩნია სათანადო გავლენის მოხდენის შესაძლებლობა.

4 ინტერპოლის მიერ გამოკვეთილი პანდემიით გამოწვეული კიბერ საფრთხეები იხილეთ ბმული:

5 კიბერდანაშაული საქართველოში (კვლევის ანგარიში), 2021, PMC Research. იხილეთ ბმული:

მოდული 2

ინფორმაციული უსაფრთხოება და ინფორმაციული აქტივების მართვა

თანამედროვე ადამიანი მე-4 ინდუსტრიული რევოლუციის ინფორმაციულ ერაში ცხოვრობს. თუკი ზოგადად განვმარტავთ, ინფორმაცია არის კონკრეტულ საკითხთან დაკავშირებული ცოდნისა და ფაქტების ერთობლიობა. ინფორმაცია არის ყველაზე მეტად ღირებული აქტივი, მას ღირებულების, სარგებლის მოტანა შეუძლია როგორც მისი მფლობელის, ასევე მომხმარებლებისთვის. მისი მატარებელი შეიძლება იყოს ფიზიკური და ელექტრონული საშუალებები – ქაღალდი, დისკი, მონაცემთა ბაზა, აუდიო და ვიზუალური მედია, მობილური, მონაცემთა ბაზა, ინტერნეტი, ინფორმაციული სისტემა. ინფორმაციული აქტივებია ყველაფერი, რაც კი მნიშვნელობის მატარებელია ორგანიზაციის თუ ინდივიდის ჭრილში – ინფორმაციული სისტემა, პროგრამული უზრუნველყოფა, კომპიუტერული ტექნიკა, ფიზიკური მოწყობილობები, თავად თანამშრომელი და მისი ცოდნა-გამოცდილება.

ინფორმაციული უსაფრთხოება არის საქმიანობა, რომელიც, უპირველეს ყოვლისა, მიმართულია ინფორმაციის, ინფორმაციული აქტივის დაცვისკენ, რათა არ მოხდეს აქტივებზე არასანქცირებული წვდომა, მათი მთლიანობის, კონფიდენციალურობისა და ხელმისაწვდომობის კომპრომეტირება, ინფორმაციულ აქტივებზე დაფუძნებული საქმიანობის შეუფერხებლად განხორციელება.

ინფორმაციულ აქტივს სამი მახასიათებელი გააჩნია, რომელთა დაცვა ინფორმაციული უსაფრთხოების მთავარი ამოცანაა. ესენია: მთლიანობა, ხელმისაწვდომობა, კონფიდენციალურობა.

• კონფიდენციალურობა – აქტივის მახასიათებელია, ის ადასტურებს, რომ აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული სუბიექტისთვის. კონფიდენციალურობის დაცვა მონაცემების გამჟღავნების პრევენციაა.

• მთლიანობა – აქტივის სიზუსტისა და სისრულის დაცვის მახასიათებელი თვისებაა. იგი მონაცემთა მოდიფიცირების პრევენციაა.

• ხელმისაწვდომობა – ავტორიზებული სუბიექტის მიერ მოთხოვნის შესაბამისად მიღებისა და გამოყენების მახასიათებელია, იგი მონაცემების არსებობის და მათზე დროული წვდომის უზრუნველყოფას აღნიშნავს.

საფრთხეები და რისკები დაკავშირებულია ინფორმაციულ აქტივებთან. საფრთხე - ქმედება, რომელმაც შესაძლოა გამოიწვიოს აქტივის კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის ხელყოფამ. საფრთხის მატარებელი შეიძლება იყვნენ თანამშრომლები და მათი არასათანადო ინფორმირებულობა/ცნობადობა, გარე ფაქტორები, ტექნოლოგიების რაოდენობისა და მასზე დამოკიდებულების ზრდა, ჰაკერული თავდასხმების, ვირუსების რაოდენობის ზრდა და მათი სირთულე, ბუნებრივი მოვლენები, მაგ.: ხანძარი, წყალდიდობა, მიწისძვრა. ხოლო სისუსტე, ეს არის ინფორმაციული აქტივის მოწყვლადი მხარე, რომელიც შეიძლება გამოიყენოს საფრთხემ და ზიანი მიაყენოს აქტივს ან ორგანიზაციას.

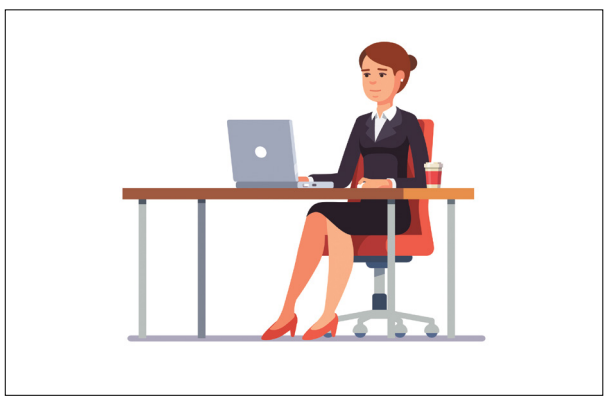
ინფორმაციული უსაფრთხოება, უპირველეს ყოვლისა, ინფორმაციულ აქტივებთან დაკავშირებული ცვალებადი რისკების მუდმივი შეფასებით, ანალიზითა და შესაძლო პრევენციული თუ მართვითი ქმედებებით არის მოცული. ინფორმაციული უსაფრთხოება მოითხოვს ინფორმაციული აქტივების კლასიფიკაციას. ინფორმაციის კლასიფიკაცია დამოკიდებულია რისკების შეფასებაზე, რომლებიც განსაზღვრავს ორგანიზაციის ზარალს მსგავსი ინფორმაციის გამჟღავნების შემთხვევაში.

ინფორმაციული აქტივების კლასიფიცირების მიზანია ინფორმაციის დაცვის სათანადო დონის უზრუნველყოფა. ინფორმაციას გააჩნია სხვადასხვა ხარისხის სენსიტიურობა და კრიტიკულობა, რაც მოითხოვს შესაბამისი დაცვის ხარისხის უზრუნველყოფას ან მოპყრობის გარკვეული წესების არსებობას. ინფორმაციის დაცვის დონე ან/და მოპყრობის მექანიზმები განისაზღვრება ინფორმაციის კლასიფიკაციის საფუძველზე.

საქართველოს კანონი „ინფორმაციული უსაფრთხოების“ შესახებ აწესებს ინფორმაციული აქტივების კრიტიკულობის ორ კლასს: კონფიდენციალური და შინასამსახურებრივი გამოყენების ინფორმაცია. საჯაროა ყველა ინფორმაციული აქტივი, რომელიც არ არის კლასიფიცირებული კონფიდენციალური და შინასამსახურებრივი გამოყენების ინფორმაციად.

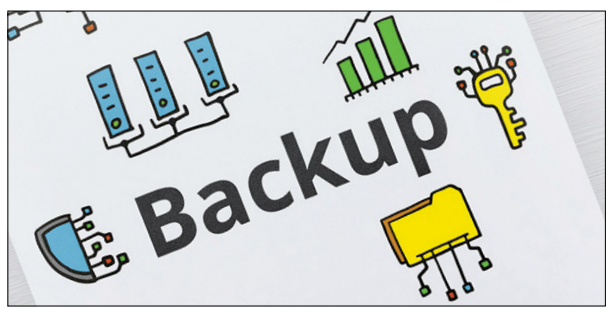
ინფორმაციული აქტივების უსაფრთხოება მოიცავს როგორც ელექტრონული, აგრეთვე ფიზიკური დაცვის ღონისძიებებს.

„სუფთა მაგიდის“ და „სუფთა ეკრანის“ პრინციპი: ნაბეჭდი მასალებისა და გადაადგილებადი მედიამატარებლებისათვის უნდა გამოიყენებოდეს სუფთა მაგიდის პოლიტიკა, ინფორმაციის დამუშავების საშუალებებისათვის კი – სუფთა ეკრანის პოლიტიკა. „სუფთა მაგიდის“ და „სუფთა ეკრანის“ პრინციპი განსაზღვრავს, როგორ უნდა მართოს ყველამ თავისი სამუშაო ადგილი და ამგვარად უზრუნველყოს ინფორმაციის უსაფრთხოება, აქტივების კონფიდენციალურობა. სენსიტიური ინფორმაცია ნებისმიერ დროს უნდა იყოს დაცული გარეშე, არასანქცირებულ პირთა წვდომისგან, იქნებიან ესენი თანამშრომლები, ოფისში მოსული სტუმრები, თუ დამხმარე პერსონალი (მაგ.: დამლაგებლები).



სარეზერვო ასლის შექმნა (მაგ.:Google Drive, iCloud-ზე) ძალიან მნიშვნელოვანია კიბერუსაფრთხოებაში, ნაწილობრივ ეს ინფორმაციის ხელმისაწვდომობის უზრუნველყოფას ემსახურება. სარეზერვო ასლის შექმნა შეიძლება იყოს ავტომატიზირებული პროცესი ან მომხმარებელი თავად ახორციელებდეს მას. თუმცა მონაცემთა შენახვის შეუზღუდავი რესურსი არ არსებობს, საჭიროა პრიორიტეტების გათვალისწინება ინფორმაციის კრიტიკულობის, მოცულობის, გამოყენების სიხშირის, თუ სხვა პარამეტრის გათვალისწინებით. სარეზერვო ასლების შექმნისას მნიშვნელოვანია მისი შენახვის ხანგრძლივობისა და დაცვის დონის (მაგ.: დაშიფვრა) განსაზღვრაც. ინფორმაციისა და პროგრამული უზრუნველყოფის სარეზერვო ასლები პერიოდულად უნდა მოწმდებოდეს ორგანიზაციაში დანერგილი პოლიტიკის შესაბამისად.

სარეზერვო ფაილები მნიშვნელოვნად იცავს მომხმარებელს მონაცემების დაკარგვისგან. ვინაიდან, ერთი მხრივ, ჩვენი კომპიუტერული მოწყობილობა შეიძლება მწყობრიდან გამოვიდეს, ფიზიკურად დაზიანდეს და ვირუსული პროგრამის გავლენით მასში დატანილი მონაცემები წაგვეშალოს. მეორე მხრივ, რენსომ-შეტევების გათვალისწინებით,მონაცემების ხელმისაწვდომობის მეტი შესაძლებლობა გვეძლევა, თუკი გვაქვს მუდმივად განახლებული სენსიტიური მონაცემების სარეზერვო ასლები.



სარეზერვო ასლის უსაფრთხოების უზრუნველსაყოფად აუცილებელია სათანადო ზომების მიღება, მათ შორის, სარეზერვო ასლების დაშიფვრა და მათზე წვდომის კონტროლის დაწესება. თუკი სარეზერვო ასლის მატარებელი დაიკარგა, მოპარულ იქნა და გატყდა, ამ შემთხვევაში უსაფრთხოების ზომების გათვალისწინებით ნაკლებია საფრთხე, რომ არაავტორიზებული პირი მოიპოვებს მონაცემებზე წვდომას.

Google Drive და iCloud არის ყველაზე პოპულარული ქლაუდ პლატფორმა მონაცემთა შესანახად. ორივეს მიმართ არაერთხელ განხორციელებულა კიბერშეტევა შენახულ მონაცემებზე წვდომის მოსაპოვებლად და მომხმარებელთა პაროლების გასატეხად.

სარეზერვო ასლის შემქმნელი საშუალებებია:

- ქლაუდ სერვისები
- პორტატული მედია
- გარე დისკები
- ლოკალური სერვერები

ინფორმაციული უსაფრთხოების უზრუნველსაყოფად გამოიყენეთ შემდეგი კარგი პრაქტიკა:

ინფორმაციული უსაფრთხოება თანამედროვე სამყაროს ყველაზე ღირებული აქტივის - ინფორმაციის დაცვას უზრუნველყოფს, იგი გახდება თქვენი ორგანიზაციის საქმიანობის განუყოფელი, თანმდევი ნაწილი.

დაიცავი ინფორმაციული აქტივი, როგორც ფიზიკური დაზიანების/განადგურებისგან, ასევე კიბერსაფრთხეებისგან. აწარმოე სარეზერვო ასლები, დაიცავი სუფთა მაგიდის/ეკრანის პრინციპი.

იზრუნე ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის შენარჩუნებაზე, მოახდინე რისკების იდენტიფიცირება, აქტივების რისკებზე დაფუძნებული მიდგომის კლასიფიცირება და თითოეულ კატეგორიაზე შესაბამისი კონტროლის მექანიზმის განსაზღვრა.

მოდული 3

პერსონალური მონაცემების უსაფრთხოება კიბერსივრცეში

ციფრული ტრანსფორმაციიის ერა ტექნოლოგიებისა და ინტერნეტის საშუალებით დიდი მოცულობის, მათ შორის, პერსონალური მონაცემების, დამუშავებით ხასიათდება. მიუხედავად მრავალი სარგებლისა, კიბერსფერო პერსონალური მონაცემებისა და პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით დღეს მსოფლიოსთვის არაერთ გამოწვევას ქმნის. კერძოდ, ტექნოლოგიური გადაწყვეტილებები ამარტივებს მოცულობითი მონაცემების შეგროვებას, ანალიზს. ხოლო ამგვარი დამუშავების გზებისა და საფუძვლების კანონიერების, სამართლიანობისა და ეთიკურობის შემოწმება სამართალდამცავებსა და Watchdog-ებს სულ უფრო და უფრო უჭირთ ტექნოლოგიური პროცესების კომპლექსურობის, გაუმჭვირვალობის და მასშტაბურობის გამო.

ინტერნეტით სარგებლობისას დაცული უნდა იყოს პირადი ცხოვრების ხელშეუხებლობის უფლება, რაც ასევე გულისხმობს პერსონალური მონაცემების, კომუნიკაციისა და კორესპონდენციის კონფიდენციალურობის დაცვას:

• ინტერნეტით სარგებლობისას პერსონალური მონაცემები მუდმივად იცვლება და მუშავდება (ელმომსახურებით სარგებლობა, ელფოსტა, სოციალური ქსელები და ა.შ.);

• საჯარო და კერძო სექტორი ვალდებულია, დაიცვას პერსონალურ მონაცემთა დამუშავების წესები;

• პერსონალურ მონაცემთა დამუშავება დასაშვებია მხოლოდ კანონმდებლობით გათვალისწინებული წესებისა და პირობების დაცვით;

• თვალთვალი და მიყურადება დაუშვებელია (გარდა კანონმდებლობით დადგენილი საგამონაკლისო შემთხვევებისა);

• პირადი ცხოვრების ხელშეუხებლობის უფლება დაცული უნდა იყოს სამუშაო ადგილზეც (ონალინ კორესპონდენციისა და კომუნიკაციის კონფიდენციალურობა)

• ქვეყანაში უნდა არსებობდეს მონაცემთა დაცვაზე პასუხისმგებელი უწყება.

ტექნოლოგური ხელშემწყობი გარემოს არასათანადოდ გამოყენებით პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დამუშავების დარღვევის ცდუნება სახელმწიფოს მხრიდანაც (არა მხოლოდ კრიმინალური დაჯგუფებების) დიდია. ტექნოლოგიები სახელმწიფო ორგანოებს უფრო მარტივად და ნაკლები კვალის დატოვებით მასობრივი თვალთვალის, მიყურადების, მონიტორინგის, ალგორითმებზე დაფუძნებული სისტემებით ელექტორატის ქცევასა თუ აზროვნებაზე დაკვირვებისა და პროგნოზირების საშუალებას აძლევს. ტექნოლოგიური სიკეთეების მანიპულირებით, შესაბამისი გარანტიებისა და სათანადო საზედამხედველო ბერკეტების არარსებობის გამო, დემოკრატიას, კანონის უზენაესობას, ადამიანის უფლებებისა და თავისუფლების დაცვას დიდი საფრთხე ექმნება.

დღევანდელ სამყაროში, როდესაც ფიზიკური პირი სულ უფრო დამოკიდებული ხდება ციფრულ ტექნოლოგიებზე, ინტერნეტსა და ელექტრონულ სერვისებაზე, ნებისმიერი მისი აქტივობა ტოვებს ციფრულ კვალს, რომლის შეგროვება, დამუშავება, შეფასება თუ ანალიზი მარტივად შესაძლებელია. არაერთი აპლიკაციის გამოყენებისთვის მომხმარებელი დამმუშავებლებს აძლევს წვდომის შესაძლებლობას ტელეფონში არსებულ ფოტოებზე, საკუთარ კონტაქტებზე, საბანკო ბარათების მონაცემებსა და სხვა მრავალ სენსიტიურ მასალაზე, რომელთა ერთობლიობა ჩვენს ციფრულ პორტრეტს ქმნის. ამ რეალობაში საკუთარი ციფრული იდენტობის მართვა ციფრული მოქალაქის უმთავრეს უნარს წარმოადგენს. როგორც ფიზიკურ სამყაროში, პირი ზრუნავს საკუთარ იმიჯზე, ანალოგიურად კიბერსივრცეში, ინტერნეტის მასშტაბის გათვალისწინებით, მეტად აქტუალური ხდება საკუთარი ციფრული რეპუტაციის შექმნა და მისი მოვლა.

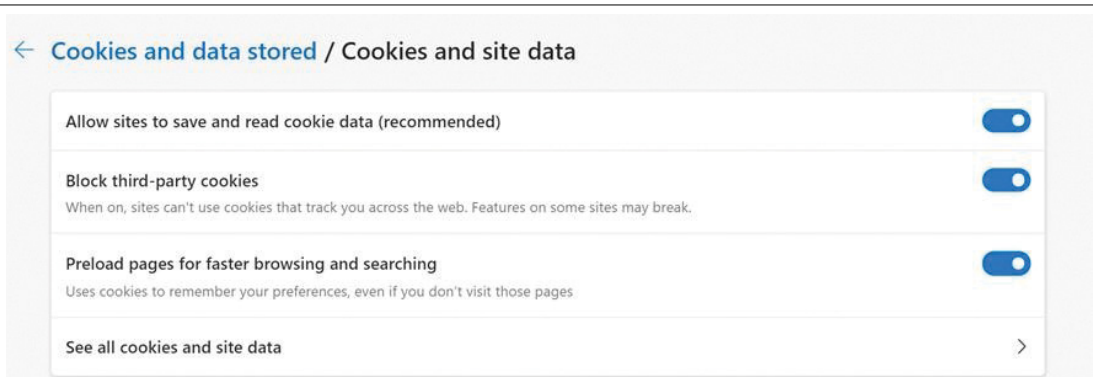
ინტერნეტი აღრიცხავს, აგროვებს და ხანგრძლივად ინახავს ყველა მომხმარებლის

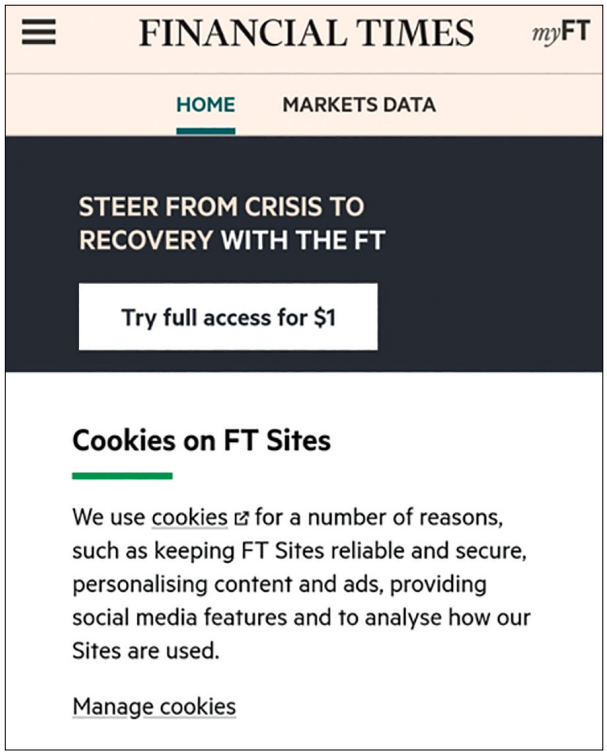
ონლაინ ქცევას, იქნება ეს ჩვენ მიერ ატვირთული ფოტოები, სხვების კომენტარები ჩვენ შესახებ, ძიების შესახებ ინფორმაცია, „ონლაინშოფინგის" ისტორია, ჩვენი ინტერესები, გადაადგილების მარშრუტი, მოგზაურობის ადგილი და აშ. ეს ყოველივე არის მომხმარებლის ონლაინრეპუტაცია. ციფრული რეპუტაცია არის ერთგვარი ციფრული კვალი, რომელსაც მომხმარებელი ტოვებს ინტერნეტში თავისი აქტივობით, ასევე ის, რასაც სხვები აქვეყნებენ მომხმარებლის შესახებ. მნიშვნელოვანია, რომ მომხმარებელმა იცოდეს ონლაინრეპუტაციის მართვა და იზრუნოს მის დაცვაზე.

საძიებო სისტემები ხელს უწყობს წვდომას დიდი მოცულობის ინფორმაციასა და ცოდნაზე, ეს საუკეთესო გზაა მომხმარებელთა შესახებ მონაცემების შესაგროვებლად, ამავდროულად, „დიდი მონაცემები" მნიშვნელოვანი გამოწვევაა პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზების პროცესში. საიტები, მაგალითად Google Search, Bing, Yahoo Search და ყველა სხვა დიდი საძიებო სისტემა, აგროვებს მომხმარებლის შესახებ მონაცემებს და იყენებს გამიზნული რეკლამების შესათავაზებლად. არ უნდა გაგვიკვირდეს, რომ რამდენიმე წუთის წინ ინტერნეტით მოძიებული პროდუქცია, სოციალურ ქსელში მყისიერად თქვენს შემოთავაზებებში გამოჩნდება, ან ახალგაცნობილ პირს იგივე Facebook-ი მეგობრებში დამატებისთვის გვთავაზობს. ინტერნეტსაძიებო სისტემებსა და ძიების შედეგებს, რომლებიც პერსონალურ მონაცემებს წარადგენს, პიროვნების დეტალური პროფილის შედგენა შეუძლია. ერთი მხრივ, თითქოსდა ამ სარეკლამო შეთავაზებებში მავნე ზეგავლენა პრაქტიკულად არაფერია, თუმცა, თუკი კარგად გავაანალიზებთ, მიზნობრივად პერსონალიზებულმა შეტყობინებებმა შეიძლება მნიშვნელოვანი ზეგავლენა იქონიოს ჩვენი გემოვნების, აზრის, ინტერესების და, მათ შორის, პოლიტიკური, სოციალური და კულტურული არჩევანის ჩამოყალიბებაზე.

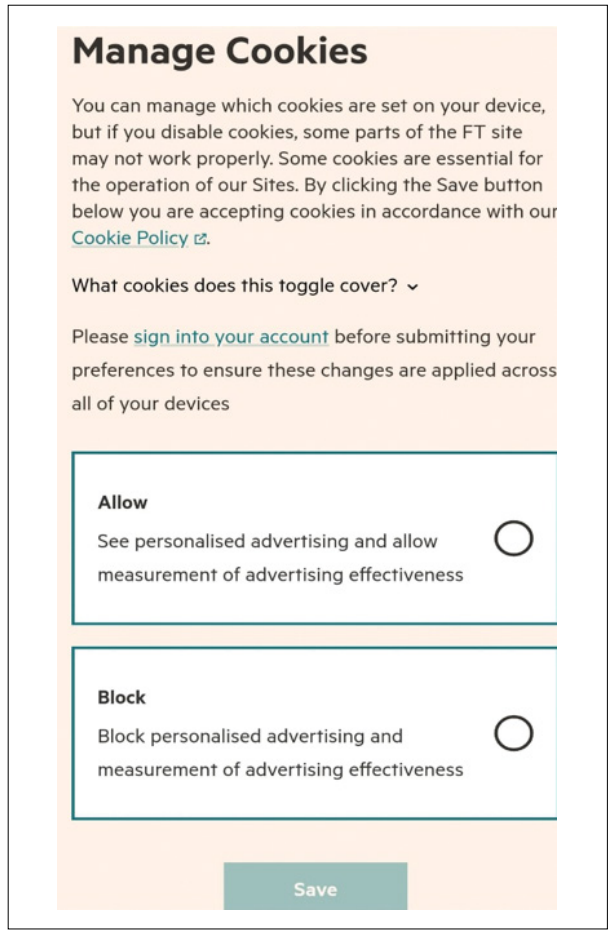
მონაცემთა სუბიექტებისათვის თავიანთი მონაცემების წაშლის/დავიწყების მოთხოვნის უფლების მინიჭება განსაკუთრებით მნიშვნელოვანია. მომხმარებელს აქვს უფლება, მოითხოვოს სოციალური ქსელის პლატფორმაზე თუ ნებისმიერ საძიებო სისტემაში გენერირებული პერსონალური მონაცემების წვდომა ან წაშლა. მაშინაც კი,როდესაც პირი თანხმობას განაცხადებს პერსონალური მონაცემების დამუშავებაზე და ინფორმაციას ატვირთავს ონლაინრეჟიმში, უნდა შეეძლოს მათი განადგურების, „დავიწყების" მოთხოვნა, თუკი სოციალური ქსელის ან სხვა ვებრესურსით მომსახურება აღარ სურს. მნიშვნელოვანია, რომ მომხმარებელს არ ევალება დასაბუთება თუ რატომ სურს მომსახურების შეწყვეტა, ეს მისი კანონიერი უფლებაა. მონაცემთა პორტირების უფლება მომხმარებლებს აძლევს საშუალებას, მიიღონ სოციალური ქსელისთვის მიწოდებული პერსონალური მონაცემების ასლი, სტრუქტურირებულ, ჩვეულებრივად გამოყენებულ, ელექტრონულ, პორტირებად ფორმატში და გადაუგზავნონ სხვა პროვაიდერს. მომსახურების გამწევი სოციალური ქსელი თუ სხვა სისტემა უნდა იყო მოქნილი რომ მყისიერად უზრუნველყოს მომხმარებლის მიერ მისი პერსონალური მონაცემების დამუშავების შეწყვეტის – წაშლის, განადგურების, პორტირების შესახებ მოთხოვნის შესრულება.

მომხმარებლები, როდესაც ინტერნეტსივრცეში ამა თუ იმ ელექტრონულ პორტალს სტუმრობენ და ინფორმაციულ-საკომუნიკაციო სერვისებით სარგებლობენ, უფლება აქვთ მოითხოვონ მონაცემთა ავტომატური საშუალებებით დამუშავების შეწყვეტა, მაგალითად „cookie" ფაილების დაბლოკვა ვებგვერდზე, ან ინტერნეტ ძიებაზე (Internet browsing) მონიტორინგის ფუნქციის გათიშვა.





„მზა-ჩანაწერების“ (Cookies) მეშვეობით ვებრესურსები აანალიზებენ მომხმარებლების ქცევას, მათ პრეფერენციებს, ინტერესებს, ახორციელებენ ქცევის პერსონალიზებას უკეთესი და მომხმარებელზე ორიენტირებული სერვისების მისაწოდებლად, თუმცა ამ პროცესში სასარგებლო ფუნქციებთან ერთად, დამმუშავებელმა ეს პერსონიფიცირებული ინფორმაცია შესაძლოა გადასცეს მესამე პირს (მაგალითად, Google) ან სხვაგვარად არამიზნობრივად დაამუშაოს პერსონალური მონაცემები, ამიტომ „მზა ჩანაწერების“ – ე.წ. „Cookie ფაილების“ დანერგვა ნებადართულია მხოლოდ მომხმარებლის თანხმობით.



თუკი სოციალური მედიის ან ნებისმიერი სხვა ინფორმაციული სისტემის წინააღმდეგ ხორციელდება კიბერთავდასხმა, შეტევა, რომელმაც შესაძლოა გამოიწვიოს ან გამოიწვია მომხმარებლების პერსონალური მონაცემების კომპრომეტირება (გაჟონვა, გამჟღავნება, წაშლა, დაკარგვა, უკანონოდ გამოყენება და აშ), მომხმარებელს აუცილებლად უნდა მიეწოდოს აღნიშნულის შესახებ გაფრთხილება.

კიბერსივრცეში პერსონალური მონაცემების დასაცავად გამოიყენეთ შემდეგი კარგი პრაქტიკა:

იზრუნეთ კარგი ციფრული იმიჯის შექმნაზე, მართეთ საკუთარი ონლაინრეპუტაცია, აღნიშნულმა შესაძლოა გავლენა იქონიოს თქვენს კარიერულ, სპორტულსა თუ პირად ცხოვრებაზე.

თუკი გაქვთ ეჭვი თქვენი ციფრული იდენტობის მითვისების, მოპარვის შესახებ, დაუყოვნებლივ შეატყობინეთ ამის შესახებ სამართალდამცავ ორგანოებს, სახელმწიფო ინსპექტორის აპარატს.

პერსონალური მონაცემების დაცვა კონკრეტული მომხმარებლის ინტერესში უნდა იყოს! კარგად დაფიქრდით რა მონაცემებს გასცემთ ამა თუ იმ საიტზე შესვლის უფლების მოსაპოვებლად, ან სხვადასხვა ონლაინ სერვისის მისაღებად - რა მიზანს ატარებს ამ მონაცემების შეგროვება, საჭიროა კი მაგალითად საცხოვრებლის მისამართის მითითება სერვისის მისაღებად?

რეგისტრაციისას განასხვავეთ სავალდებულო და არასავალდებულო ველები ინფორმაციის შესაყვანად. არ დაამახსოვრებინოთ საბანკო მონაცემები.

დარწმუნდით ვებგვერდის ავთენტურობაში, რომელზეც რეგისტრირდებით ან რომლის მომსახურებასაც იყენებთ, იმისთვის რომ არ მოხდეს პერსონალური მონაცემები არასანდო პირთა ხელში.

არ უპასუხოთ ელექტორნულ გზავნილებს, რომელშიც მოთხოვნილია თქვენი პერსონალური ინფორმაცია. (მაგ.: მომსახურების გაუმჯობესებისთვის გამოგვიგზავნეთ თქვენი საბანკო ბარათის რეკვიზიტები).

მოდული 4

ინტერნეტი და მისი უსაფრთხოდ გამოყენება

ინტერნეტი საჯარო მომსახურების ღირებულების მატარებელია. ადამიანები, საზოგადოება, საჯარო დაწესებულებები და კერძო კომპანიები საკუთარი საქმიანობის განხორციელებისას ინტერნეტზე არიან დამოკიდებული. მათ ლეგიტიმური მოლოდინი აქვთ, რომ ეს სიკეთე ფიზიკურად და ფინანსურად ხელმისაწვდომი, უწყვეტი, სანდო და დაცული იქნება ყოველგვარი დისკრიმინაციისაგან. გარდა ამისა, მომხმარებლებს აქვთ ლეგიტიმური ნდობა, რომ ინტერნეტის გამოყენებისას ადამიანის უფლებათა და ძირითად თავისუფლებათა რეალიზაციისას დაცული იქნება მატერიალურ/ოფლაინს-ამყაროში მოქმედი სტანდარტები, არავინ დაექვემებარება არამართლზომიერ, ზედმეტ და არათანაზომიერ ჩარევას.

ინტერნეტთან წვდომის შეზღუდვა დაუშვებელია, გარდა იმ შემთხვევებისა, როდესაც კანონამდებლობით გათვალისწინებული წესით ამას სასამართლო ადგენს. ინტერნეტი ყოველგვარი დისკრიმინაციის გარეშე უნდა იყოს ხელმისაწვდომი, მათ შორის ფინანსურადაც. მომხმარებელს მაქსიმალური წვდომა უნდა გააჩნდეს ინტერნეტის კონტექსტისადმი, აპლიკაციებისა და სერვისებისადმი სასურველი ტექნიკური მოწყობილობის გამოყენებით. სახელმწიფო ხელისუფლება უნდა ატარებდეს გონივრულ ზომებს, რათა ინტერნეტი ხელმისწვდომი იყოს მუნიციპალურ დონეზე, გეოგრაფიულად მოშორებულ ტერიტორიებზე, დაბალი შემოსავლის ან/და სპეციალური საჭიროებების, შეზღუდული შესაძლებლობების მქონე პირებისათვის.

დღესდღეობით ინტერნეტის ყველაზე პოპულარული გამოყენება ვებსაიტების მონახულება-დათვალიერება/სტუმრობაა, რაც მობილური მოწყობილობების, სხვადასხვა გაჯეტების და კომპიუტერის საშუალებით ხდება. ვებბრაუზინგში იგულისხმება ინტერნეტგვერდებზე შესვლა, მონახულება, სერვისებით სარგებლობა, ინფორმაციის მიღება და კომუნიკაცია, ანუ ინტერნეტსივრცეში ჩვენი ყველა აქტივობა. ყველაზე ფართოდ ცნობილი ვებბრაუზერებია: Microsoft Edge, Mozilla Firefox, Google Chrome, Apple's Safari, Opera, მათ ჩვენ ყოველდღიურ ცხოვრებაში ვიყენებთ. ინტერნეტბრაუზინგს განსაკუთრებული ყურადღება ეთმობა კიბერუსაფრთხოებაში. კერძოდ, როგორ გავხადოთ ჩვენი ინტერნეტსაძიებო სისტემებში, ვებრესურსებში შესვლა და მათი გამოყენება უსაფრთხო, ისე რომ არ გავხდეთ კიბერშეტევების მსხვერპლი– ეს არის ვებრესურსებით უსაფრთხო სარგებლობის მიზანი.

როგორ ვისარგებლოთ ინტერნეტრესურსით უსაფრთხოდ და დაცულად? მართალია 100%-ით უზრუნველყოფა პრაქტიკულად შეუძლებელია, თუმცა რამდენიმე მნიშვნელოვანი მექნიზმი ამ საქმეში მაინც გვეხმარება.

ძირითადად რა საფრთხეს ვაწყდებით ვებრესურსებით სარგებლობისას? უპირველეს ყოვლისა, როგორც ნებისმიერ ინფორმაციულ სისტემას, ვებგვერდებსაც და აპლიკაციებსაც, მათ პროგრამულ უზრუნველყოფას ტექნოლოგიური სისუსტეები/ ხარვეზები ახასიათებს. ამ მოწყვლადობებს კი ჰაკერები მომხმარებლებზე თავდასხმისთვის, მათ სისტემებში შეღწევისა და არასანქცირებული აქტივობებისთვის იყენებენ. მაგალითად, ძალიან გავრცელებულია ინფიცირებული ვებგვერდები, ე.წ. „გატეხილი" რესურსები, რომელზე სტუმრობისას მომხმარებელი ინფიცირდება, მაგალითად ხდება მისი პერსონალური მონაცემების დაუფლება, მომხმარებლის იდენტობის მოპარვა და ა.შ. ფიშინგი ვებრესურსებით სარგებლობისას ფართოდ გავრცელებული საფრთხეა.

ინტერნეტში ბრაუზინგის დროს ვებსაიტზე „ამოხტება" ხოლმე ე.წ. popup ფანჯარა, რომელიც გვთხოვს, რომ დავაკლიკოთ რაიმე ღილაკს ან/და გადმოვწეროთ რაიმე პროგრამა, რომელიც ხშირ შემთხვევაში „ვირუსია. ასევე ხშირია შემთხვევები, როდესაც უცნობ ლინკზე დაკლიკებისას გადმოიწერება მავნე ფაილი, ისე რომ ეს ვერ შევამჩნიოთ და რაღაც დროის მერე ეს აღმოჩენილი ფაილი

ჩვენს კომპიუტერში გავუშვათ. რაც საბოლოო ჯამში შესაძლებელია ვირუსი იყოს და თქვენ გახდეთ დაინფიცირების მსხვერპლი.

ფიშინგი კიბერთაღლითობის გავრცელებული ფორმაა, იგი შესაძლოა განხორციელდეს როგორც ელექტრონული ფოსტის გაგზავნით, ასევე ბრაუზინგის დროსაც. ფიშინგის მიზანია მსხვერპლის მოტყუება, „ანკესზე წამოგება“ და ამ გზით სენსიტიური ინფორმაციის დაუფლება ან მომხმარებლის კომპიუტერული სისტემის კომპრომეტირება. ვებბრაუზინგის დროს ხშირად შეგხვდებათ ვებსაიტი, რომელიც მიმსგავსებულია ნამდვილ ვებსაიტს, ყალბ ვებსაიტზე მომხმარებლის და პაროლის შეყვანისას ჰაკერი ეუფლება მომხმარებლის პერსონალურ, მათ შორის, საბანკო ინფორმაციას. ინტერნეტ-ფიშინგის შემთხვევაში კრიმინალი გამოგიგზავნით შეტყობინებას, რომ მეილსერვერზე მიმდინარეობს სამუშაოები და თქვენი ელექტრონული ანგარიში რომ არ წაიშალოს, აუცილებლად უნდა მიაწოდოთ თქვენი მომხმარებლის სახელი ან პაროლი.

ვინაიდან ინტერნეტში ბევრი არასანდო ვებრესურსია, დიდი ტექნოლოგიური ვენდორიები ცდილობენ მომხმარებელს შესთავაზონ მათი ამოცნობის მარტივი გზები. მაგალითად, კომპანია Google - მა შეიმუშავა სტრატეგია თუ როგორ დაეცვა Google Chrome - ის მომხმარებლები სანდო და არასანდო რესურსების გარჩევის გზით. ამისთვის შემუშავდა HTTPS და HTTP სტრატეგია. თუკი მომხმარებელი შევა საიტზე, რომელსაც არ აქვს მხარდაჭერა დაცული HTTPS კავშირის, მაშინ ბრაუზერი დაუწერს, რომ იგი იმყოფება დაუცველ საიტზე შეტყობინებით: “Not Secure” – მისამართის მარცხენა მხარეს.

HTTPS კავშირი ნიშნავს, რომ თქვენ მიერ განხორციელებული ინტერნეტ კავშირი/კომუნიკაცია უსაფრთხოა და დაცულია შიფრაციით. HTTPკავშირი კი ნიშნავს საპირისპიროს. მიუხედავად იმისა, რომ HTTPS ზრდის საიტის უსაფრთხოებას, ეს არ ნიშნავს, რომ ჰაკერებს არ შეუძლიათ მისი გატეხა.

განსაკუთრებით მნიშვნელოვანი საშუალებაა, თუ თქვენი ბრაუზერი ამოწმებს ვებგვერდის საწყის კოდს და გატყობინებთ ვებგვერდი ინფიცირების თაობაზე. ამ ფუნქციას იყენებენ ისეთი ინტერნეტბრაუზერები როგორიცაა: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari და Opera.

ვებრესურსების არასანდოობას, სიყალბეს რამდენიმე ნიშნის არსებობა შეიძლება ადასტურებდეს:

• გრამატიკული, ორთოგრაფიული შეცდომებით არასწორად შედგენილი წინადადებები;

• საიტით სარგებლობისთვის გადაჭარბებული რაოდენობის პერსონალური ან კონფიდენციალური ინფორმაციის გამჟღავნების მოთხოვნა.

• ბმულები, რომლებიც გადაგამისამართებენ უცნობ საიტზე ან საიტზე, რომელიც ცნობილი საიტის ანალოგია, თუმცა მისამართში მცირედი ცვლილებებია.

• ინფორმაციის შეყვანისას ახალი გახსნილი ვებ-გვერდი არ არის დაკავშირებული მთავარ გვერდთან, რომლის მომსახურებით თუ პროდუქტით სარგებლობისთვისაც ავსებთ ამ მონაცემებს.

• ვებგვერდზე გამოდის შეტყობინება „under construction”.

• “@” სიმბოლოს არსებობა გვერდის URL გვერდზე, როგორც წესი, მიუთითებს თაღლითური ვებგვერდის არსებობაზე.

ინტერნეტით უსაფრთხოდ სარგებლობის კარგი პრაქტიკა:

ვებბრაუზერის განახლება – იმისათვის, რომ მაქსიმალურად შევამციროთ მოწყვლადობის პირობა, საჭიროა, ვსარგებლობდეთ ბოლო, განახლებული ვერსიებით, რომლებშიც უკვე გასწორებულია აღმოჩენილი სისუსტეები.

სიფრთხილით მოეკიდეთ HTTP საიტებს და ყურადღება მიაქციეთ „Not Secure" შეტყობინებას.

ნუ გადმოწერთ უცხო საიტებიდან პროგრამებს, ამით შეიძლება დაავირუსოთ თქვენი კომპიუტერული მოწყობილობა.

გადაამოწმეთ საიტების სანდოობა სპეციალური სერვისებით, სანამ ისარგებლებთ და შეიყვანთ მათზე თქვენს მონაცემებს.

გამოიყენეთ უსაფრთხო კავშირი მისამართის ზოლში, მისამართი უნდა დაიწყოს https: // და გამოსახული უნდა იყოს ბოქლომის ნიშანი.

ნუ გამოყენებთ ერთი და იმავე ონლაინ ავთენტიფიკაციის მონაცემებს სხვადასხვა ვებრესურსებისთვის.

ნებისმიერი ელ.ფოსტის მისამართი, რომელიც სრულდება დაბოლოებით: „ru" საფრთხის შემცველია ინფორმაციული უსაფრთხოების კუთხით, განსაკუთრებით კი საჯარო მოხელეებისათვის (მაგალითად: giorgi@rambler.ru, ana@mail.ru და ა.შ.). ამიტომ, აუცილებელია, თუ გაქვთ მსგავსი ელ.ფოსტის მისამართი, დაუყოვნებლივ შეცვალოთ ახალით.

მოდული 5

ელექტრონული ფოსტის უსაფრთხოება

ელექტრონული ფოსტით სამსახურებრივი და პირადი მიზნით სარგებლობა, კომუნიკაცია და კორესპონდენციის წარმოება, თავისი სისწრაფით, მოქნილობითა და სტრუქტურირებით, ძალიან ფართოდ გავრცელებული სერვისია. შესაბამისად, ამ სერვისზე კიბერშეტევებიც არახალია, მომხმარებლებისთვის კი აუცილებელია ელფოსტით კომუნიკაციისას მასთან დაკავშირებული რისკებისა და შესაბამისი დამცავი ზომების სათანადოდ გაცნობიერება.

ყოველდღიურად ელფოსტით არაერთ წერილს ვიღებთ და ვაგზავნით. დღესდღეობით ელფოსტის ტრაფიკის 90% სპამია, ყოველდღიურად 30 მილიონი სპამმესიჯი იგზავნება უმეტესწილად აშშ-დან, ვიეტნამიდან, ინდოეთიდან, ჩინეთიდან, მექსიკიდან, რუსეთიდან, საფრანგეთიდან, ბრაზილიიდან, გერმანიიდან და თურქეთიდან. ყოველ სამ წერილში ერთი წარმოადგენს არასასურველს ჩვენთვის და არის რისკის მატარებელი მომხმარებლისთვის.

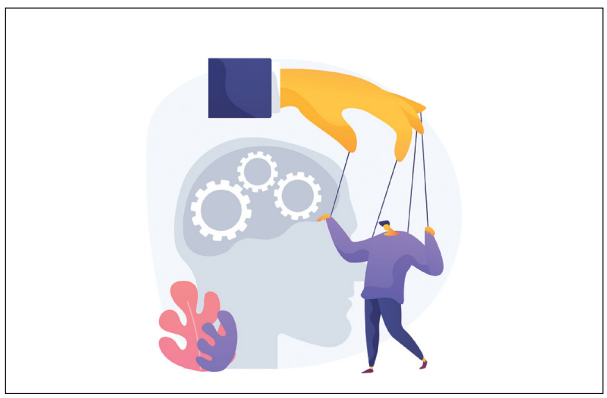
სამწუხაროდ, ელფოსტით ვიღებთ არასასურველ და არასაჭირო მესიჯებსაც. ელფოსტით მომსახურებას უსაფრთხოების თვალსაზრისით მრავალი სისუსტე აქვს: არაავტორიზებული წვდომა მონაცემებზე, მონაცემების კომპრომეტირება, ელექტრონული ფოსტის წყაროს ანუ გამგზავნის მონაცემების გაყალბება. სამწუხაროდ, ჰაკერები ელფოსტას იყენებენ მომხმარებლების შეცდომაში შეყვანის და მათი მონაცემების დაუფლების მიზნით. ელ-ფოსტით სარგებლობისას ძირითადი საფრთხეებია: სპამი, სარეკლამო/მარკეტინგული წერილები, ფიშინგი, საეჭვო ბმულები, მავნე ჰიპერლინკები და ფაილები, ინფორმაციის გაჟონვა ელფოსტით კომუნიკაციისას, სოციალური ინჟინერია, ელფოსტის აპლიკაციები.

SPAM მესიჯები, ჩვეულებრივ, ეგზავნება მომხმარებელთა ფართო ჯგუფს. გარდა იმისა, რომ ისინი მომხმარებელს აკარგვინებენ დროსა და რესურსს, ასევე გამოიყენება ფიშინგის, რეკლამის, ვირუსის ან მავნე ფაილების გასავრცელებლად. სპამთან გასამკლავებლად გამოიყენება ელფოსტის სპამფილტრები, რომელთაც თქვენი ელფოსტის კლიენტებზე შეუძლია ამოიცნოს სპამმეილები.

ელფოსტით განხორციელებულ კიბერშეტევებს შორის ფიშინგი ერთ-ერთი ყველაზე პოპულარულია. წერილი წარმოდგენილია როგორც სანდო წყაროსაგან მიღებული შეტყობინება. იგი შენიღბულია როგორც სასწრაფო შინაარსის მესიჯი, რომელშიც დამატებითი ინფორმაციისთვის მოთავსებულია ბმულები ან მიმაგრებულია დოკუმენტები. ფიშინგმეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად ხდება მსხვერპლის კომპიუტერში შეღწევა ან მისგან დამატებითი პერსონალური ინფორმაციის მოპოვება (პაროლი, მომხ-

მარებლის სახელი, ბარათის ინფორმაცია და სხვა). კიბერ-დამნაშავეები ცდილობენ ფიშინგმეილები დააგზავნონ მასობრივად, სპამმეილის ფორმით, მეტ ადრესატთან, რაც მათი წარმატების ალბათობას მაქსიმალურად ზრდის.

ჩვეულებრივ, სტანდარტული მომხმარებელი, როგორც წესი, ბოლომდე არ კითხულობს მიღებულ კორესპონდენციას და დაუფიქრებლად ხსნის ელფოსტით მიღებულ ბმულს ან თანდართულ ფაილს. როგორც ბმული, ასევე ფაილი ხშირ შემთხვევაში ინფიცირების დიდი რისკის მატარებელია და სოციალური ინჟინერიისთვის გამოიყენება.



სოციალური ინჟინერია უსაფრთხოების კონტექსტში მომხმარებლებზე მანიპულირების, მათი მონაცემების და ღირებული აქტივების დაუფლების, კრიტიკულ სისტემებში შეღწევის მიზნით გამოიყენება. ამ შემთხვევებში შეტევის სამიზნე-მსხვერპლი არის - მომხმარებელი და არა კომპიუტერული სისტემა.

როგორ გავხადოთ ელფოსტით კომუნიკაცია უსაფრთხო, მისი კონფიდენციალურობა, ხელმისაწვდომობა და მთლიანობა უზრუნველყოფილი? უსაფრთხოების მრავალ ფაქტორს შორის მნიშვნელოვანია (End-to-End დაშიფვრა, უსაფრთხოების პროტოკოლები, Hop-by-Hop დაცვა). End-to-end დაშიფვრა (E2EE) არის კომუნიკაციის უსაფრთხო მეთოდი, რომელიც აბრკოლებს მესამე-არასანქცირებული მხარის მიერ კომუნიკაციის მონაცემებზე წვდომას, მონაცემების ერთი სისტემიდან მეორე მოწყობილობაში გადაგზავნის დროს. E2EE-ში მონაცემები დაშიფრულია გამგზავნის სისტემასა ან მოწყობილობაზე და მხოლოდ მის ადრესატს შეუძლია გაშიფვრა/წაკითხვა. ელფოსტით კომუნიკაციის დროს E2EE ადასტურებს წერილის გამომგზავნის ავთენტურობას, რომ წერილის შინაარსის გაჟონვა (მათ შორის სერვერების მხრიდან) არ მომხდარა კომუნიკაციის განხორციელების პროცესში. სტანდარტულად, პოპულარული ელფოსტის სერვისები, როგორიცაა: Gmail და Outlook, არ გულისხმობს დაშიფვრის სერვისს, თუმცა ის ხელმისაწვდომია ყველა თანამედროვე მეილპროვაიდერისთვის. მაგალითად PGP (Pretty Good privacy) მეთოდი, რომელიც საშუალებას იძლევა, წერილები დაშიფროთ (გამოყენებულია ციფრული ხელმოწერა, ღია გასაღები) და მხოლოდ მიმღებმა გახსნას თავისი კუთვნილი მისამართით.

ელექტრონული ფოსტით უსაფრთხოდ სარგებლობის კარგი პრაქტიკა:

ელფოსტის აპლიკაციები გადმოწერეთ სანდო წყაროებიდან, რათა თავიდან აიცილოთ მავნე პროგრამული უზრუნველყოფის, ვირუსების გავრცელება თქვენს სისტემებში.

ელფოსტის აპლიკაციები მუდმივად განაახლეთ, რათა უსაფრთხოების უახლესი პარამეტრებით იყოთ აღჭურვილი.

არ გადახვიდეთ სპამმეილში შემოთავაზებულ ბმულებზე, არ გახსნათ ფაილები, წერილის დანართები.

არ გახსნათ უცნობი პირისგან გამოგზავნილი წერილები, მიმაგრებული ფაილები, ბმულები, მათ შორის ნაცნობი პირისგან მიღებული წერილები, საეჭვო ბმულებითა და ფაილებით.

არ გააგზავნოთ ელფოსტით კონფიდენციალური ინფორმაცია, ან თუკი აგზავნით დოკუმენტი/ფაილი დაშიფრეთ, დაადეთ კოდი.

პერიოდულად ამოწმეთ თქვენს ელფოსტაზე განხორციელებული აქტივობები და ელფოსტის პაროლი, ხომ არ არის გატეხილი ელფოსტის ანგარიში.

არ დაარეგისტრირო სამსახურებრივი ელფოსტა სხვადასხვა საიტებზე, ფორუმებსა და სოციალურ ქსელზე საკომუნიკაციო/საკონტაქტო წყაროდ.

საეჭვო წერილის, ბმულის, დოკუმენტის მიღების შემთხვევაში, არ ჩამოტვირთო ისინი კომპიუტერში ან არ გადაუგზავნო სხვას, არამედ დაუკავშირდი უსაფრთხოების სამსახურს.

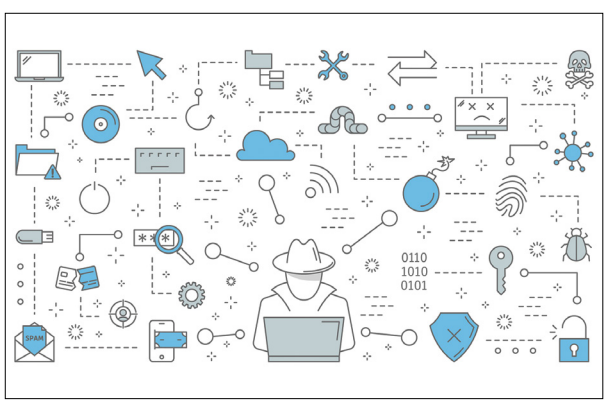
დარწმუნდით, რომ ელფოსტის სერვერები და მისი კლიენტები სარგებლობენ უსაფრთხო პროტოკოლებით, რომლებიც მოიცავს ავტორიზაციისა და დაშიფვრის თანამედროვე მეთოდებს.

მოდული 6

პერსონალური კომპიუტერის უსაფრთხოება

პერსონალური კომპიუტერი არის საბოლოო მომხმარებლის მიერ საკუთარი ინტერესებით/საჭიროებებით შერჩეული (ზომა, შესაძლებლობები, ფასი და სხვა მახასიათებლები) ზოგადი დანიშნულების კომპიუტერი, რომელსაც ვიყენებთ სამსახურებრივი თუ პირადი მიზნებისთვის. პერსონალური კომპიუტერი შეიძლება იყოს დესკტოპის კომპიუტერი ან ლეპტოპი, ნეტბუქი, პლანშეტი და ა.შ. მნიშვნელოვანია აღინიშნოს, რომ თუკი ათეული წლების წინ კიბერკრიმინალების მთავარი სამიზნე დესკტოპ კომპიუტერი იყო, ამჟამად ტექნოლოგიურ განვითარებასთან ერთად სამიზნეთა წრეც გაფართოვდა. ჩვენ დღეს უფრო მეტ ოპერაციას ლეპტოპებსა და ტაბლეტებზე ვასრულებთ, ამიტომ სწორედ ეს მოწყობილობებია საფრთხის მთავარი მატარებელი.

პერსონალური კომპიუტერის წინააღმდეგ კიბერსაფრთხის წყარო სხვადასხვაგვარია. ჩვენი კომპიუტერი შეიძლება დაინფიცირდეს არალეგიტიმური წყაროებიდან პროგრამული უზრუნველყოფის და ოპერაციული სისტემების განახლებებით, რომლებიც ვირუსის მატარებელია, პირატული პროდუქტებით, აგრეთვე პორტატული მეხსიერების ბარათებიდან, მავნე, არასანდო საიტებზე სტუმრობით, ელფოსტით მიღებული წერილებით, სხვადასხვა ბმულებისა და დოკუმენტების/ფაილებისა და მედია საშუალებების გახსნა-ჩამოტვირთვით, ანტივირუსული პროგრამებით, სოციალური მედიასაშუალებებით და ა.შ.



მავნე კოდისთვის პროგრამული უზრუნველყოფის მრავალი ფორმა, სახეობა და გავრცელების მექანიზმი არსებობს. მაგალითად: ტროიანები (Trojans), ე.წ. უკანა კარი (Backdoors), ლოგიკური ბომბები (Logic Bombs), ვირუსები (Viruses), ჭიები (Worms). მალვეარი მოიცავს კომპიუტერულ ვირუსებს, ასევე რენსომვეარს. კომპიუტერულ ჭიას შეუძლია გამოიყენოს საფრთხეები და ავტომატურად გამრავლდეს კომპიუტერსა და მის ქსელში. ხოლო ტროიანი არის პროგრამა, რომელიც თითქოს უსაფრთხოა და ლეგიტიმურ ფუნქციებს ასრულებს, მაგრამ ამავდროულად მალავს საზიანო ფუნქციებსაც. ჭიებსა და ტროიანებს შეუძლიათ დააზიანონ პერსონალური კომპიუტერის სისტემის მონაცემები ან ამ კომპიუტერის გამართულად მუშაობა.

მავნე კოდის შესახებ ცნობილი, ფართოდ გავრცელებული მაგალითებია სტაქსნეტი, მირაი ბოტნეტი, Crypto Ransomware.

პერსონალურ კომპიუტერზე მუშაობის პროცესში ვიყენებთ სხვადასხვა ოპერაციულ სისტემას (Windows, MacOS, Linux, Android, iOS), უამრავ პროგრამას თუ აპლიკაციას. შესაბამისად ძალიან მნიშვნელოვანია, რომ სისტემები და პროგრამები გადმოვწეროთ სანდო ვებგვერდებიდან და იყოს სანდო კომპანიების მიერ შექმნილი, ლიცენზირებული და განახლებული. პერსონალური კომპიუტერის უსაფრთხოების თვალსაზრისით ერთ-ერთი ყველაზე მნიშვნელოვანი წესია რეგულარულად განახლებული პროგრამული უზრუნველყოფის გამოყენება. ეს ეხება ოპერაციულ სისტემას, აპლიკაციებს, საოფისე პროგრამებს და მედიასაშუალებებს. როგორც წესი, ძირითადი ტექნოლოგიური ვენდორები და პოპულარული პროგრამები სთავაზობენ ავტომატური განახლების მექანიზმებს და პერიოდულად ატყობინებენ მომხმარებელს. აქვე მნიშვნელოვანია, ყურადღებით ვიყოთ საეჭვო ბანერებსა და შეტყობინებებთან, რომლებიც გვთავაზობენ განახლების ჩამოტვირთვას

და დაინსტალირებას. როგორც წესი, ასეთი განახლებები მოიცავს მავნე კოდებს და იწვევს ჩვენი კომპიუტერის დაინფიცირებას.

სხვადასხვა ფორუმებსა და ტორენტებზე განთავსებული პროგრამები შეიძლება იყოს საფრთხის შემცველი პერსონალური კომპიუტერისა და მასში დაცული კრიტიკული, სენსიტიური ინფორმაციისთვის. პირატული პროგრამებიც გავრცელებული საშუალებაა ვირუსის გასავრცელებლად.

მაგ.: პირატული პროგრამები ლეგიტიმურ პროგრამას “Skype.exe” ფაილს მიაბავენ მავნე კოდს, “Skype”-ის გაშვების შემდეგ მავნე კოდი გაეშვება სკაიპთან ერთად.

ანტივირუსული პროგრამები იცავს პერსონალურ კომპიუტერს (სრულყოფილი დაცვა შეუძლებელია) მავნე პროგრამებისა და საზიანო აპლიკაციებისგან. ანტივირუსის მთავარი ფუნქციაა პერსონალურ კომპიუტერში აღმოაჩინოს მავნე ფაილები და საზიანო აპლიკაციები.

ინტერნეტსივრცეში საკმაოდ ბევრი განსხვავებული ფუნქციის ანტივირუსია ხელმისაწვდომი. ანტივისურით სარგებლობისას მის შერჩევასთან ერთად ყველაზე მნიშვნელოვანია მისი სწორი გამოყენება – სისტემატური განახლება, კომპიუტერში არსებული ფაილების პერიოდული სკანირება.

დღესდღეობით ყველა კომპიუტერს გააჩნია USB პორტი, რომლის საშუალებითაც შეგვიძლია გამოვიყენოთ USB მეხსიერების ბარათი. USB მეხსიერების ბარათი თავისი პორტატულობის, მოქნილობისა და ტევადობის გათვალისწინებით აქტიურად გამოიყენება მომხმარებლებში, თუმცა მას უსაფრთხოების თვალსაზრისით თავისი რისკებიც გააჩნია: შესაძლებელია კიბერკრიმინალებმა მომხმარებლისგან მალულად USB პორტში შეაერთონ მავნე USB მეხსიერება და ასე

დაეუფლონ პერსონალრ კომპიუტერში დაცულ კრიტიკულ სენსიტიურ ინფორმაციას. ასევე USB დისკზე შეიძლება იყოს ვირუსი, რომელიც გააქტიურდება მისი გამოყენებისთანავე.

მონაცემთა არასანქცირებული ტრანსფერი ინსაიდერების (შიდა საფრთხის აქტორების) მიერ ხშირად პორტატული მოწყობილობების მეშვეობით ხორციელდება, როდესაც ისინი USB მეხსიერების ბარათებით კლასიფიცირებული კორპორატიული ქსელებიდან იპარავენ საიდუმლო დოკუმენტაციას.

მარტივი სიტყვებით რომ ვთქვათ, firewall დამცავი ფარის როლს ასრულებს და პერსონალურ კომპიუტერსა და მის კერძო ქსელს იცავს ინტერნეტის არასანქცირებული წვდომისგან.

Firewalls არის შემომავალი და გამავალი ქსელის ტრაფიკის შეზღუდვის/კონტროლის ეფექტური მეთოდი და თუ სწორად არის კონფიგურირებული, ხელს უშლის მრავალი კიბერთავდასხმის განხორციელებას. ამასთან, განსაკუთრებით საინტერესოა კორპორაციული გარემოსათვის, Firewall ასევე ზღუდავს გამავალ ტრაფიკს და, სათანადო კონფიგურაციის შემთხვევაში, მონაცემთა ექსფილტრაციისგან დაცვას უზრუნველყოფს.

პერსონალური კომპიუტერით უსაფრთხოდ სარგებლობის კარგი პრაქტიკა:

არ გამოიყენოთ რუსული ანტივირუსული პროდუქტები მაგ: „Kaspersky“. გამოიყენეთ მაგალითად „Windows defender”-ი.

მნიშვნელოვანი მონაცემები დაიცავი პაროლით, ყველაზე მარტივი მეთოდია დოკუმენტებზე პაროლის დაყენება ან მათი პაროლით დაცულ ზიპ ფაილში ჩადება.

არ ჩამოტვირთოთ ფაილები, განახლებები ტორენტგვერდებიდან, ისინი შესაძლოა მავნე კოდების შემცველი იყოს. არ ისარგებლოთ ტორენტული გვერდებით.

შეგიძლიათ გამოიყენოთ მყარი დისკის შიფრაცია და თქვენი პაროლის გარეშე ვერავინ მიიღებს წვდომას თქვენს პერსონალურ კომპიუტერზე. მაგალითად, Microsoft-ის სისტემისთვის გამოიყენე Bltlocker-ი.

პერსონალურ კომპიუტერზე მუშაობისას, სანამ დავტოვებდეთ სამუშაო ადგილს, აუცილებელია კომპიუტერის დაბლოკვა. გამოიყენე Ctrl+Alt+Delete.

არ შეაერთოთ უცნობი/შემთხვევით აღმოჩენილი USB ბარათი თქვენს კომპიუტერში. ასევე არ შეინახოთ USB ბარათში სენსიტიური ინფორმაცია, სამსახურებრივი მონაცმეები.

გამოიყენეთ ინფორმაციული და კიბერუსაფრთხოების სხვადასხვა მექანიზმებისა და საშუალებების კომბინირება (ანტივირუსი, ფაიარვოლი, განახლება და აშ) სათანადო დონის დაცულობის მისაღწევად.

მოდული 7

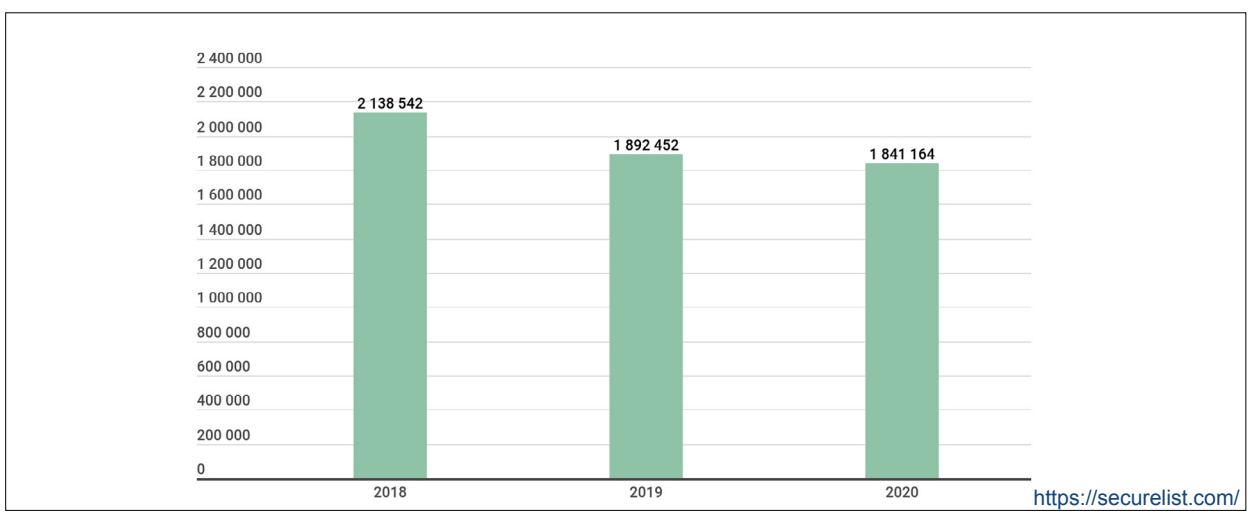
მობილური მოწყობილობების უსაფრთხოება

21-ე საუკუნე ტექნოლოგიური რევოლუციის ხანაა. კლასიკური ტექნოლოგიები, როგორიცაა პერსონალური კომპიუტერი სხვადასხვა, მეტად მობილური მოწყობილობებითა და მოქნილი ტექნოლოგიური გადაწყვეტილებებით იცვლება. სულ უფრო და უფრო იზრდება მობილური მოწყობილობების მოხმარება, მობილური ტელეფონის აპლიკაციების მოხმარების ზრდასთან ერთად იზრდება მათთან დაკავშირებული კიბერსაფრთხეებიც. მობილური მოწყობილობების სიკეთეები ვერ მოიტანს შესაბამის სარგებელს, თუკი ამ ტექნოლოგიებთან დაკავშირებული საფრთხეები არ იქნა დაძლეული. მაგალითად, მაკაფის ლაბორატორიული კვლევების მიხედვით, მსოფლიოში მობილურ მოწყობილობებთან დაკავშირებული მალვეარი/მავნე პროგრამული უზრუნველყოფა 2016 წელთან შედარებით 5-ჯერ გაიზარდა. მობილურ მოწყობილობებში არსებული მალვეარი გამოიყენება ბოტნეტების, მობილური მონაცემების მოპარვის, კიბერჯაშუშობისა და მიზნობრივი კიბერთავდასხმების განსახორციელებლად. 2020 წელი მობილური მოწყობილობების საშუალებით განხორციელებული ფარული კიბერშეტევების წლად დასახელდა. როგორც კიბერდამნაშავეებმა, ასევე თავად სახელმწიფოებმა აქტიურად გააფართოვეს მობილური შეტევების ვექტორი დაწყებული Backdoor-ებით დამთავრებული კრიპტოვალუტების მოპოვებით.

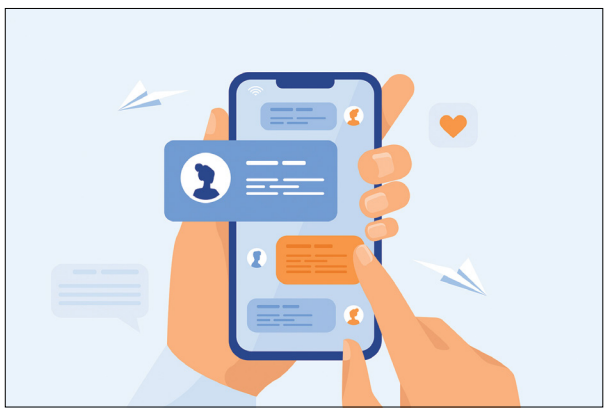
თუკი ადრე ყველაფერს ვაკეთებდით კომპიუტერით, დღეს თითქმის ყველაფერი გადაინაცვლებს მობილურ სმარტტელეფონებზე, შესაბამისად, მობილური მოწყობილობების ფიზიკური მოვლა და ინფორმაციული/კიბერუსაფრთხოება მსოფლიოს ყველა მომხმარებლისთვის კრიტიკულად მნიშვნელოვანია.

სმარტმობილური მოწყობილობები მსოფლიოში ყველაზე გაუმჯობესებული სათვალთვალო საშუალებას წარმოადგენს. როგორც კი თქვენი სმარტფონის აპლიკაციების გამოყენებისას ადგილმდებარეობის მონაცემებს აზიარებთ, მისი წაშლა ან უკან გამოხმობა შეუძლებელია. ბევრი აპლიკაცია, რომელიც გთხოვთ ადგილმდებარეობის მითითებას, მაგალითად ამინდის, სავაჭრო ან ადგილობრივი სიახლეების აპლიკაციები, ხშირად მის გარეშეც მშვენივრად მუშაობენ. არ არსებობს მიზეზი იმისთვის, რომ მაგალითად, ამინდის აპლიკაციას, დასჭირდეს ზუსტი ადგილმდებარეობა თქვენთვის ამინდის პროგნოზის მოსაწოდებლად. Apple-მა ბოლო დროს საკმაოდ გაართულა კომპანიებისთვის

მსოფლიო მასშტაბით მობილურ მოწყობილობებთან დაკავშირებული მალვეარის სტატისტიკური მონაცემები



თქვენი ადგილმდებარეობის გამოცნობა ისეთი მეთოდების გამოყენებით, როგორებიცაა ახლომდებარე Bluetooth და Wi-Fi ქსელები. დარწმუნდით, რომ თქვენი სმარტმოწყობილობის ინფორმაციული სისტემა განახლებულია, რათა ისარგებლოთ უსაფრთხოების ამ მეთოდებით. გაითვალისწინეთ, თუ თქვენ გჭირდებათ ისეთი აპლიკაციებით სარგებლობა, როგორიცაა Foursquare, Google Maps, Apple Maps, და ა.შ. მაშინ ზემოხსენებული სერვისების დროებით ჩართვა მოგიწევთ. iOS-ზე ადგილმდებარეობის ამოცნობის გამოსართავად, ეწვიეთ Apple's location services support page (ეფლის ადგილმდებარეობის მხარდამჭერ გვერდს). ანდროიდის შემთხვევაში, უბრალოდ შედით ტელეფონის პარამეტრებში, შემდეგ „ადგილმდებარეობაში“ და გამორთეთ ყველა ოფცია.



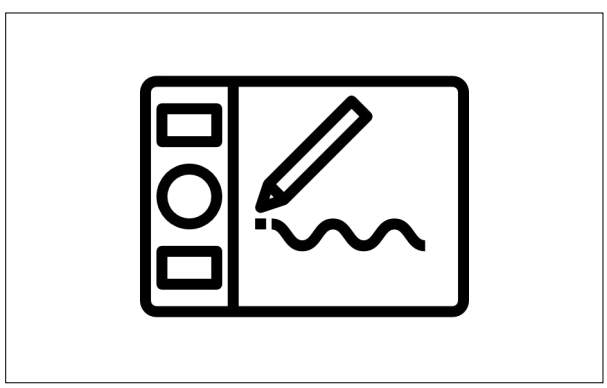
დღეს სმარტფონების ბუმია და მილიონობით ადამიანისთვის მობილური სმარტფონი ან მოწინავე შესაძლებლობების მქონე მობილური ტელეფონი ფასდაუდებელი საშუალებაა. გაყიდული სმარტფონების რაოდენობა ყოველწლიურად იზრდება 2007 წლიდან (122,3 მილიონი) და 2017 წლამდე (1,53 მილიარდი). მობილური მოწყობილობების შესაძლებლობები პრაქტიკულად უსასრულოა. სმარტფონები და პერსონალური ციფრული ასისტენტები (PDA) მომხმარებლებს აძლევენ კავშირს ელექტრონულ ფოსტაზე, ინტერნეტზე, GPS ნავიგაციაზე და ბევრ სხვა პროგრამაზე, სმარტფონები ასევე სამხედრო საკომუნიკაციო სისტემებშიც კი გამოიყენება.

სმარტმოწყობილობები კიბერშეტევებისთვის უფრო და უფრო მიმზიდველი სამიზნე ხდება, მათი მზარდი პოპულარობის გამო. ბოლოდროინდელი გამოკითხვების თანახმად, ინფორმაციული უსაფრთხოების პროფესიონალების მესამედზე მეტი თვლის, რომ მობილური მოწყობილობები ყველაზე დიდ საფრთხეს შეუქმნის მათ ორგანიზაციებს უახლოეს მომავალში, სოციალურ ქსელებსა და ქლაუდ ტექნოლოგიებთან ერთად. მობილურ მოწყობილობებთან დაკავშირებული კიბერსისუსტეებია: საფრთხის შემცველ Wi-Fi-ზე წვდომა, დაკარგული ან/და დაზიანებული მოწყობილობები, მობილურ ოპერაციულ სისტემებზე შეტევა. ამ მოწყვლადობებთან დაკავშირებული საფრთხეები იზრდება, „გამოიყენეთ თქვენი პირადი მოწყობილობები (Bring Your Own Device)“ შეთანხმებების პოპულარობის გამოც.

მოიტანეთ თქვენი საკუთარი მოწყობილობა (სმარტფონები, ტაბლეტები, ლეპტოპები, USB) არის ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც ორგანიზაციის თანამშრომლებს საშუალებას აძლევს გამოიყენონ თავიანთი პერსონალური მოწყობილობები სამუშაოსთან დაკავშირებული საქმიანობისთვის: ელფოსტასთან წვდომა, კორპორაციულ ქსელთან დაკავშირება, კორპორაციული აპლიკაციებისა და მონაცემების გამოყენება.

ხშირ შემთხვევაში მობილურ მოწყობილობებთან დაკავშირებით მომხმარებელი უფრო ნაკლებად იყენებს უსაფრთხოების ზომებს, ვიდრე პერსონალურ კომპიუტერთან მიმართებით, რაც, რა თქმა უნდა, არასწორი პრაქტიკაა. მობილური მოწყობილობების უსაფრთხოების უზრუნველყოფისთვის გვჭირდება ყველა ის მექანიზმი (და უფრო მეტიც), რომელიც პერსონალურ კომპიუტერთან დაკავშირებით არის მოთხოვნილი, მაგალითად: ანტივირუსი, პროგრამებისა და აპლიკაციების განახლება, სარეზერვო ასლების წარმოება, უსაფრთხოების კონფიგურაცია, ფაიარვოლი და ა.შ. საყურადღებოა, რომ ხშირ შემთხვევაში თქვენი კომპიუტერული სამუშაო სივრცის დაცვაში თუკი უსაფრთხოების და ტექნიკური პერსონალი მონაწილეობს, მობილური მოწყობილობებით სარგებლობისას, ჰაკერების პირისპირ ხშირად ჩვეულებრივი მომხმარებელი რჩება.

მობილური ოპერაციული სისტემის უსაფრთხოება. იმის გამო, რომ მოსახლეობის თითქმის 100% იყენებს Android და iOS სისტემებს, კიბერკრიმინალები მუდმივად ეძიებენ ახალ მოწყვლადობებს ამ სისტემებში, რათა გამოიყენონ ახალი შეტევისთვის. მნიშვნელოვანია, რომ ჩვენი მობილური ტელეფონების ოპერაციული სისტემები მუდმივად განახლებულ მდგომარეობაში გვქონდეს.



მობილური მოწყობილობების ფიზიკური უსაფრთხოება. ვინაიდან მობილური მოწყობილობა პორტატულია და მარტივია მისი დაკარგვა, აუცილებელია მისი ფიზიკური უსაფრთხოების უზრუნველყოფა. აშშ-ის ინფორმაციული უსაფრთხოების სპეციალისტების ჯგუფში ჩატარებული გამოკითხვა ცხადყოფს, რომ კორპორაციების კონფიდენციალური და სენსიტიური მონაცემების კომპრომატირების ერთ-ერთი ყველაზე გავრცელებული გზა თანამშრომელთა მიერ სმარტმოწყობილობების დაკარგვაა. მნიშვნელოვანია, რომ ბლუთუსის სერვისი გამოიყენება ფარული მიყურადების, DDoS შეტევისა და მალვეარით ინფიცირებისთვის.

მობილური აპლიკაციების რაოდენობა ყოველდღიურად იზრდება. სამწუხაროდ, არც თუ იშვიათია შემთხვევები, როდესაც ჰაკერები მიაკვლევენ უსაფრთხოების თვალსაზრისით მოწყვლად მხარეებს ამა თუ იმ სანდო აპლიკაციაში, ჩააშენებენ მასში მალვეარს და ამით მართავენ სხვადასხვა მობილურ აპლიკაციას. მაგ.: ელფოსტის ფუნქციების, სმს-ების, ხმოვანი შეტყობინებებისა და GPS ლოკაციის კონტროლის.

მობილური მოწყობილობებით უსაფრთხოდ სარგებლობის კარგი პრაქტიკა:

განაახლეთ თქვენი Android და iOS სისტემები, პერიოდულად შეამოწმეთ განახლების შედეგი.

როდესაც არ სარგებლობთ მობილურით, ყოველთვის დაბლოკილ მდგომარეობაში იქონიეთ იგი.

დაკარგული ტელეფონის შემთხვევაში, გამოიყენეთ Find my phone აპლიკაცია ლოკაციის დასადგენად.

გადმოწერთ აპლიკაციები მხოლოდ ავტორიზებული წყაროებიდან, ნუ ენდობით უცხო მესამე წყაროებს.

ნუ გექნებათ Bluetooth-ი ჩართული, თუ მას არ იყენებთ.

დაშიფრე მობილურ მოწყობილობებში შენახული მონაცემები და ამით აირიდე არასანქცირებული წვდომა. აწარმოე სარეზერვო ასლები.

მოდული 8

უკაბელო ქსელებით უსაფრთხოდ სარგებლობა

ბოლო ათწლეულის მანძილზე ინტერნეტკავშირისთვის უკაბელო ქსელებით სარგებლობა პოპულარული გახდა მოქნილობის გამო, ვინაიდან არ არის საჭირო კაბელების გაყვანა, მათზე წვდომა მარტივია, პორტატულია, გამოსაყენებლად მოსახერხებელია მომხმარებლებისთვის. საზოგადოებრივი თავშეყრის ადგილებში – რესტორნები, სასტუმროები, ბარები, ბიბლიოთეკები, აეროპორტები ამ ტექნოლოგიას ანიჭებენ უპირატესობას. მომხმარებლების უმრავლესობა უერთდება სრულიად უცნობ ინტერნეტ ქსელებს, რადგან ისინი ღია და უფასოა.

საჯარო, ღია და დაუცველი ქსელები ჰაკერების ოპერირებისთვის ერთ-ერთი პოპულარული სივრცეა. მათთვის ძალიან მარტივია ღია ქსელში კომპიუტერულ მოწყობილობაზე შეტევა, ამავდროულად მისი აღმოჩენა ძალზედ რთულია. უკაბელო ქსელები, როგორც წესი, იყენებენ სამაუწყებლო რადიო გადაცემის საშუალებებს. სამაუწყებლო კომუნიკაციისას გადაცემულ მონაცემებზე წვდომა შეუძლია ნებისმიერს ქსელის დაფარვის ზონაში. შესაბამისი ტექნოლოგიური მოწყობილობებითა და პროგრამული უზრუნველყოფით შესაძლებელია გადაცემის მონაცემების მიღება, გენერირება, გადაცემისთვის ხელის შეშლა.

ჰაკერს შეუძლია ღია ქსელიდან მოიპოვოს წვდომა მომხმარებლის პირად ან სამსახურებრივ მონაცემებზე. ღია ქსელები საუკეთესო სივრცეა მომხმარებლების ინფორმაციის მოსაპარად. როდესაც შედიხარ სისტემაში (“Logging in”) შენი პირადი ინფორმაციის დაცულობა რისკის ქვეშაა. არც თუ იშვიათად, ჰაკერები ქმნიან ღია ქსელებს, რათა მომხმარებლების საშუალებით ადვილად გაავრცელონ ვირუსები მათ მოწყობილობებში და დაეუფლონ ინფორმაციას, იქნება ეს სხვადასხვა ვებ გვერდებზე შესასვლელი რეკვიზიტები, ინტერნეტ ნავიგაციისას განხორციელებული აქტივობები, საბანკო ბარათებისა და ფინანსური ტრანზაქციების შესახებ ინფორმაცია და ა.შ.

ერთ-ერთი გავრცელებული ტექნიკაა ინტერნეტში შესასვლელი კოდის სანაცვლოდ მომხმარებლის პერსონალური მონაცემების შევსება (ტელეფონის ნომერი, ელფოსტა) ან მომხმარებლის გადაყვანა Facebook გვერდზე, რომელიც თითქმის რეალურად გამოიყურება, თუმცა როგორც კი ამ „თითქმის რეალურ“ საიტზე მოხვდება პირადი მონაცემები, ისინი უკვე მესამე პირისთვის ხელმისაწვდომი ხდება.

უკაბელო ქსელებით, ჰოტსპოტებით სარგებლობასთან დაკავშირებული გავრცელებული საფრთხეებია მოსმენა/მიყურადება (eavesdropping), ქსელით ინფორმაციის გადაცემის ჩახშობა (jamming the network), ჩაწერილი შეტყობინებების გამეორება (replay of recorded messages), ყალბი შეტყობინებები (bogus messages), ნებისმიერი სხვა შეტევა, რომელიც ტრაფიკის ანალიზის შედეგად ხორციელდება. ერთ-ერთი ყველაზე პოპულარული შეტევა არის სნიფინგი (sniffing). ჰაკერს აქვს შესაძლებლობა sniffing - ის მეშვეობით ქსელში გაცვლილი ინფორმაცია უკანონოდ, არასანქცირებულად დაათვალიეროს. ინტერნეტში არსებობს უამრავი სნიფერული, მავნე პროგრამა. სნიფინგიდან ყველაზე საუკეთესო დაცვაა end-to-end ან user-to-user ტრაფიკის შიფრაცია.

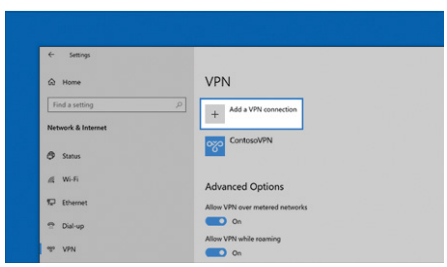
ვირტუალური კერძო ქსელი (VPN – ვირტუალურ კერძო ქსელთან დასაკავშირებლად მომხმარებლის კავშირის დაშიფვრა) არის ტექნოლოგია, რომელიც თავდაპირველად შეიქმნა დისტანციურად მყოფი თანამშრომ-

ლებისთვის სამსახურებრივ ქსელში სამუშაოდ, თუმცა შემდგომ მისი მოხმარების წრე გაფართოვდა უსაფრთხოების მიმართ მზარდი ინტერესის გათვალისწინებით. როდესაც ვიმყოფებით ღია სივრცეში და ვიყენებთ უცხო Wi-Fi ქსელს, VPN ტექნოლოგია უზრუნველყოფს ჩვენსა და ნებისმიერ ვებ-რესურსს შორის უსაფრთხო და დაცულ კავშირს. მისი გამოყენება შესაძლებელია როგორც მობილური ტელეფონებიდან, ასევე კომპიუტერული ტექნოლოგიების საშუალებით. სანდო VPN–ის გარეშე ნებისმიერი ინფორმაცია, რომელსაც მომხმარებელი ცვლის საზოგადოებრივ WI-Fi–ზე, შეიძლება იყოს დაუცველი. ეს შეიძლება იყოს

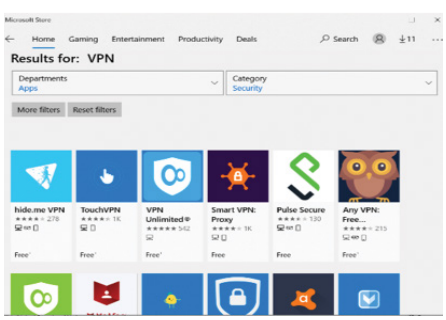
თქვენი სოციალური მედიის მონაცემები, საბანკო ანგარიშის რეკვიზიტები, საკრედიტო ბარათების ნომრები და ა.შ.

VPN პროფილის შექმნა (Windows 10)

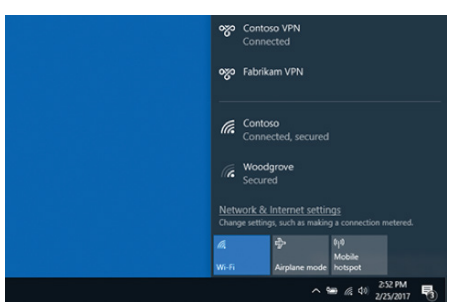
VPN კავშირის დამყარებამდე, მომხმარებლის მოწყობილობაზე საჭიროა VPN პროფილის კონფიგურირება.



სამსახურეობრივი მიზნებისთვის, როგორც წესი ორგანიზაციის ინფორმაციულ ტექნოლოგიური დეპარტამენტი წინასწარ აინსტალირებს მომხმარებლის მოწყობილობაზე ავტორიზებული VPN აპლიკაციას და აკონფიგურირებს მას ორგანიზაციის უსაფრთხოების პოლიტიკების მიხედვით.



პირადი სარგებლობისთვის, მომხმარებელს შეუძლია ეწვიოს Microsoft Store-ს, შეარჩიოს და დაინსტალიროს საკუთარ მოწყობილობაზე სასურველი VPN აპლიკაცია.



VPN კავშირის დასამყარებლად დააჭირეთ, შეარჩიეთ სასურველი VPN კავშირი და დააჭირეთ Connect.

უკაბელო ქსელის გამოყენებისას უსაფრთხოების კარგი პრაქტიკა:

საჯარო უკაბელო ქსელთან დაკავშირებისას, გაითვალისწინეთ, რომ იგი საიმედოდ დაცული არ არის, ამიტომ თავი შეიკავეთ მონაცემების და ინფორმაციის გაცვლისგან.

ღია უკაბელო ქსელებით სარგებლობისას მოერიდეთ სენსიტიური ინფორმაციის ინტერნეტ ბანკისა და ელ-ფოსტის, სოციალური ქსელების გამოყენებას.

შეამოწმეთ თქვენი მოწყობილობის პარამეტრები: გამორთეთ ავტომატურად Wi-Fi-ი ქსელთან დაკავშირების შესაძლებლობა.

ნუ გამოიყენებთ უცხო ან/და უპაროლო Wi-Fi-ის.

გამოიყენეთ რთული პაროლი და პერიოდულად ცვალეთ იგი თქვენი Wi-Fi-ი როუტერისთვის.

დარწმუნდით თქვენი მოწყობილობის სისტემის განახლებაში და ინტერნეტით ნავიგაციისას გამოიყენეთ მხოლოდ დაცულ პროტოკოლზე – https ვებ-რესურსები.

გამოიყენეთ VPN რესტორნებში, აეროპორტებში, სასტუმროებში. იგი დაგეხმარებათ ინტერნეტ ბრაუზინგის პროცესში ინფორმაციისა და პერსონალური მონაცემების დაცვაში.

მოდული 9

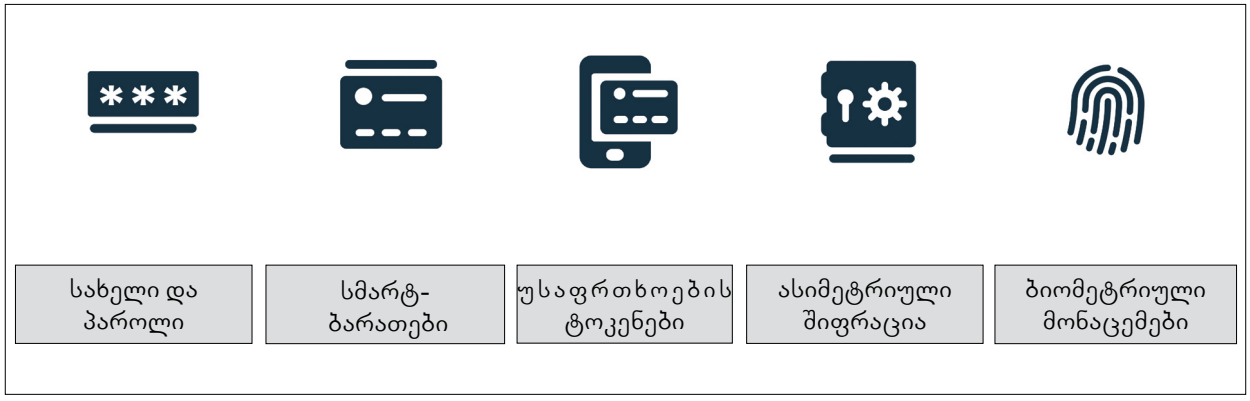
პაროლების უსაფრთხოება და მართვა

ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების განვითარებამ შესაძლებელი გახადა საჯარო და კერძო სერვისების მოდერნიზაცია, მათზე მომხმარებლის წვდომის გაზრდა, რამაც მნიშვნელოვანი გავლენა იქონია ციფრული მმართველობის, ელექტრონული კომერციის განვითარებაზე, ეკონომიკურ წინსვლასა და სოციალური პრობლემების დაძლევაზე. სერვისების „გაციფრულება“ მნიშვნელოვნად ზოგავს დროს, ფინანსურ და ადამიანურ რესურსებს. ამავდროულად ელექტრონული სერვისებით სარგებლობა შეიცავს უსაფრთხოებასთან დაკავშირებულ რისკებს, რაც გულისხმობს კიბერშეტევებსა და ონლაინ თაღლითობის შესაძლებლობებს. საჯარო თუ კერძო სერვისების დისტანციურად, ელექტრონულ ფორმატში მიწოდება საჭიროებს მომხმარებლების უსაფრთხო იდენტიფიცირებისა და ავთენტიფიკაციის მექანიზმების არსებობას.

უსაფრთხო ელექტრონული ავთენტიფიკაცია არის პროცესი, რომლითაც დგინდება მომხმარებლის მიერ ელექტრონულად წარმოდგენილი მონაცემების სანდოობა. ეს მომსახურება ხშირად გამოიყენება სხვადასხვა სერვისის მიმწოდებლების მხრიდან მომხმარებელთა და მათ ავტორიზაციაზე ინფორმაციის მართვის მიზნით. ონლაინ ავთენტიფიკაცია შეიძლება იყოს მარტივი - ერთდონიანი ან ორ და მრავალდონიანი.

მრავალფაქტორიანი ავთენტიფიკაციის დროს მომხმარებელს ეძლევა წვდომა ვებ-საიტზე ან პროგრამაში მხოლოდ ორი ან მეტი მტკიცებულების ავტორიზაციის მექანიზმში წარმატებით წარდგენის შემდეგ. ავთენტიფიკაციისთვის საჭირო მონაცემები, როგორც წესი, უკავშირდება კონკრეტული მონაცემების ცოდნას, ინფორმაციის ან მოწყობილობის ფლობას. ავთენტიფიკაციის ფართოდ გავრცელებული მაგალითებია ავტორიზაცია სახელისა და პაროლის კომბინაციით, უსაფრთხო ტოკენები, ასიმეტრიული შიფრაციის მეთოდი, სმარტ-ბარათები, ბიომეტრიული მონაცემები. სამწუხაროდ, ინფორმაციული სისტემების უმრავლესობა არ იყენებს მრავალდონიან ავთენტიფიკაციას, თუმცა ეს ტენდენცია იცვლება.

ინფორმაციულ სისტემაზე ავტორიზაციის პროცესში ყველაზე ხშირად ვიყენებთ სახელისა და პაროლის კომბინაციას. პაროლი არის სხვადასხვა სიმბოლოების ერთობლიობა, რომელიც მომხმარებლის ანგარიშს იცავს არასანქცირებული, მესამე პირების წვდომისგან. პაროლი შესაძლებელია ჰქონდეს ნებისმიერ კომპიუტერულ მოწყობილობას, იქნება ეს Desktop კომპიუტერი, მობილური ხელსაწყოები, ლეპტოპები, ტაბლეტები თუ მეხსიერების ბარათები. პაროლებზე შეტევის ცნობილი მაგალითებია ონლაინ და ოფლაინ Dictionary Attack & Brute Force Attack (კრიმინალი ცდილობს სხვადასხვა პაროლების კომბინაციების გამოყენებით გატეხოს მომხმარებლის პაროლი) შეტევები. პაროლებზე

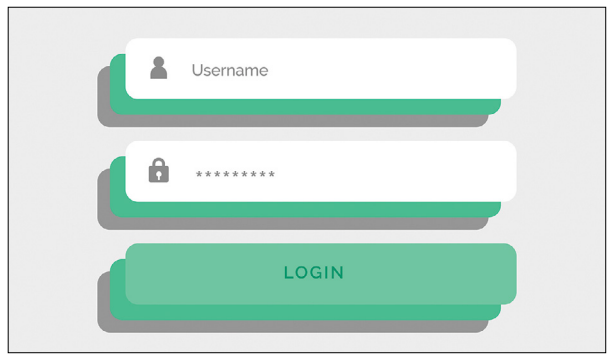


წვდომის მოპოვება ხდება ფიშინგ შეტევებით, ტროიანებით, მავნე ფაილებით. Keylogger ასევე ფართოდ გავრცელებული ჯაშუში პროგრამული უზრუნველყოფაა, რომელიც აკონტროლებს მომხმარებლის თითოეულ ღილაკზე დაჭერის ფაქტს და კონკრეტული კომპიუტერის კლავიატურაზე მოქმედებებს. Keylogger პროგრამის დაინსტალირება შესაძლებელია რამდენიმე წამში და ინსტალაციის შემდეგ ჰაკერს შეუძლია მსხვერპლის პაროლის მიღება.

მიუხედავად იმისა, რომ ტექნოლოგიებმა ჩვენი ცხოვრება უნდა გაამარტივონ, დაზოგონ ჩვენი დრო და ენერგია, ამ სიმარტივის გამოყენება პაროლებთან დაკავშირებით არასასურველია. რაც უფრო მარტივია პაროლი, მით მეტი რისკის შემცველი და პოტენციური პრობლემის მომტანია მომხმარებლისთვის. პაროლი უნდა იყოს რთული და შეიცავდეს მინიმუმ 8 სიმბოლოს, ციფრებს, დიდ და პატარა ასოებს, სხვადასხვა სიმბოლოს, არ უნდა უკავშირდებოდეს მომხმარებლის პერსონალურ მონაცემებს და მასთან დაკავშირებულ მოვლენას.

დიდი ბრიტანეტის ეროვნულმა კიბერ უსაფრთხოების ცენტრმა (NCSC), ჩაატარა გამოკითხვა და შეკრიბა იმ პაროლების სია, რომელსაც მომხმარებლები ყველაზე ხშირად იყენებდნენ. პაროლი: „123456“ გამოიყენებოდა 23.2 მილიონი მომხმარებლის მიერ, შემდგომ მოდის „123456789“ პაროლი, რომელსაც 7.7 მილიონი მომხმარებელი ყავს.

უნიკალური პაროლებით სარგებლობა და მათი დადგენილი პერიოდულობით განახლება არ არის მარტივი ჩვეულებრივი მომხმარებლისთვის. ამ საქმიანობის გასა-



მარტივებლად გამოიყენება პაროლების მართვის სისტემები. ამ შემთხვევაში მომხმარებელი ვალდებულია დაიმახსოვროს მხოლოდ მართვის სისტემის პაროლი, ხოლო სისტემა ყველა მითითებული გვერდისთვის თვითონ დააგენერირებს რთულ პაროლს. გარდა იმისა, რომ იგი იმახსოვრებს უამრავი ვებსაიტის პაროლებს, იგი ავტომატურად ავსებს პაროლის ველებს მხოლოდ ლეგიტიმურ ვებსაიტებზე.

პაროლების გამოყენებისას უსაფრთხოების კარგი პრაქტიკა:

ნუ დაუშვებთ რომ თქვენმა ვებბრაუზერმა (FireFox, Chrome, Safari, Opera, IE, Microsoft Edge) შეინახოს თქვენი პაროლები, რადგან ვებბრაუზერებში შენახული ყველა პაროლი ადვილად შეიძლება იქნას გატეხილი.

პერიოდულად ამოწმეთ თქვენი პაროლები კომპლექსურობაზე არსებული ინტერნეტრესურსების გამოყენებით.

პერიოდულად ამოწმეთ გატეხილია თუ არა თქვენი პაროლი შესაბამისი ინტერნეტრესურსების გამოყენებით.

თუკი მომხმარებლისთვის რთულია კომპლექსური პაროლის მოფიქრება, შესაძლებელია პაროლების ავტომატური გენერაციის სისტემით სარგებლობა.

გამოიყენეთ თითოეულ სისტემაზე – უნიკალური პაროლი.

პაროლები უნდა ვცვალოთ დადგენილი პერიოდულობით.

მოდული 10

სოციალური ქსელებით უსაფრთხოდ სარგებლობა

ინტერნეტის განვითარებამ დასაბამი მისცა თანამედროვე სამყაროს უმნიშვნელოვანეს კულტურულ და ტექნოლოგიურ რევოლუციას – სოციალური მედიის გაჩენას. ბოლო 10 წლის განმავლობაში ონლაინ სოციალური მედიის გეოგრაფიული არეალი, მოხმარების მასშტაბები სწრაფად გაიზარდა და ასობით მილიონი ადამიანის მოღვაწეობის სივრცედ იქცა. სოციალური ქსელები კომუნიკაციის, ინფორმირებულობის, აზრის გამოხატვის, დოკუმენტების გაზიარების, სოციუმში აქტიური მონაწილეობის მნიშვნელოვანი და პოპულარული მექანიზმებია. სოციალური ქსელები ონლაინ კომუნიკაციის პლატფორმებია, სადაც ადამიანები რეგისტრირდებიან ან ქმნიან თანამოაზრეთა ქსელს. სოციალური პლატფორმები, როგორიცაა Facebook, Twitter, WhatsApp, Pinterest, Instagram და Google Plus ოჯახთან, მეგობრებთან და სოციუმთან მუდმივად კონტაქტზე ყოფნის შესაძლებლობას იძლევა. ზოგიერთი სოციალური მედია, როგორიცაა LinkedIn, Skype, Slack ასევე მნიშვნელოვანი მექანიზმებია ჩვენი პროფესიული საქმიანობისა და ბიზნეს ქსელის გასაფართოებლად.

ქსელში გასაწევრიანებლად ან შესაქმნელად ადამიანებმა უნდა წარმოადგინონ პერსონალური მონაცემები და შექმნან საკუთარი პროფილი. სოციალური ქსელები მომხმარებლებს აძლევს ციფრული „კონტენტის“ გენერირების საშუალებას, რაც შეიძლება მოიცავდეს ფოტოებსა და ვიდეოებს, საგაზეთო ბმულებსა და პერსონალურ პოსტებს საკუთარი მოსაზრებების გამოსახატავად. ონლაინ კომუნიკაციის პლატფორმების საშუალებით მომხმარებლებს შეუძლიათ ინტერაქცია და კომუნიკაცია. სოციალური ქსელების უმრავლესობაზე რეგისტრაცია უფასოა. სოციალური ქსელები შემოსავალს იღებენ მიზანმიმართული რეკლამებიდან. რეკლამის განმთავსებლები დიდ სარგებელს ხედავენ სოციალურ ქსელებში ყოველდღიურად გამჟღავნებული პერსონალური მონაცემებისგან. ინფორმაცია მომხმარებელთა ასაკის, სქესის, ადგილმდებარეობისა და ინტერესების შესახებ მათ საშუალებას აძლევს რეკლამებით სამიზნე აუდიტორიას მიწვდნენ.

ელ.ფოსტის მისამართები, რომლებიც სრულდება დაბოლოებით „ru“ განსაკუთრებით საფრთხის შემცველია, რადგანაც მსგავს ელ.ფოსტაზე განთავსებული ნებისმიერი ინფორმაცია სრულად ექვემდებარება რუსეთის ფედერაციის კონტროლს, როგორც პრაქტიკული წვდომის კუთხით (ნებისმიერი მსგავსი ელ.ფოსტა რუსეთის სერვერებზეა განთავსებული) ისე სამართლებრივად ექვემდებარება რუსეთის ფედერაციის კანონმდებლობას, რაც მათ აძლევს შესაძებლობას ნებისმიერი ფორმით შეაღწიონ თქვენს კუთვნილ ელ.ფოსტასა და მასზე განთავსებულ მონაცემებზე.

ზოგიერთი სტატისტიკა:

ყოველთვიურად 3,30 მილიარდზე მეტი ადამიანი იყენებს Facebook, Instagram, WhatsApp ან Messenger-ს.

Facebook-ს ყოველთვიურად 25,5 მილიარდი ვიზიტორი ჰყავს, რაც მას ყველაზე მეტად პოპულარულ ვებგვერდებს შორის მესამე ადგილს ანიჭებს (Google– ისა და YouTube– ის შემდეგ).

Facebook-ი არის საშუალო სტატისტიკური ამერიკელებისთვის ინფორმაციის/სიახლეების მიღების ტიპური წყარო.

ინდუსტრიული ბიზნესის მიერ სოციალური ქსელების პერსონალურ მონაცემების შეუსაბამო, გადაჭარბებული შეგროვება და გამოყენება ჩვენთვის არასასურველი ობიექტური რეალობაა. ხშირად ამ მონაცემებს ისინი მომხმარებლებისგან შესაბამისი ინფორმირების გარეშე იღებენ. ეს შეიძლება მოხდეს არაერთი წყაროს (პირდაპირი მარკეტინგი, გამოყენებული ვებ-გვერდები, გადმოწერილი აპლიკაციები, ადგილმდებარეობის მონაცემები და სხვა მარავალი) გამოყენებით.

დადებითი კონტექსტი

კავშირის დამყარება/განახლება, საჯარო მონაწილეობა, ჩართულობა, სხვადასხვა ღონისძიებებისა და მოვლენების, ახალი ტენდენციების ცენტრში ყოფნა, გართობითი ხასიათი, საჯარო ხილვადობა/საქმიანობის აფიშირება, რეკლამირება, კოლექტიურად აზრის თვითგამოხატვა, შეკრება.

უარყოფითი კონტექსტი

ალტერნატიული სინამდვილე/ფაქტები, არასწორი, ცრუ ინფორმაცია, ტროლები და ბოტები, ბულინგი და სიძულვილის ენა, დანაშაულის/კიბერდანაშაულის ჩადენის პლატფორმა, მავნე ფსიქოლოგიური ზეგავლენა, გადაჭარბებული დამოკიდებულება, პერსონალურ მონაცემებსა და პირად ცხოვრებაზე არამიზნობრივი მონიტორინგი, თვალთვალი, ონლაინადევნება, მასების რადიკალიზაცია, ტერორიზმსა და ორგანიზებულ დანაშაულში მომხმარებლების მობილიზება.

სოციალური ქსელები მსოფლიოს მასშტაბით სახის ამომცნობ უდიდეს მონაცემთა ბაზებს ფლობენ, რომლებსაც როგორც საბაზრო საქონელს ისე იყენებენ. მაგ.: უზიარებენ მესამე პირებს, მარკეტინგულ კომპანიებს, ვენდორებს. სოციალური ქსელების მომხმარებლები ყოველდღიურად დაუფიქრებლად აზიარებენ საკუთარ ან სხვა მომხმარებლების ფოტოებს შესაბამისი თეგებით (tags), ეს ინფორმაცია სოციალური მედიის მაგნატებს უფრო და უფრო მეტი სიზუსტით პირის ვიზუალური იდენტიფიცირების საშუალებას აძლევს. თითქოს უწყინარი აუდიო-ვიზუალური მასალის გაზიარებით დაინტერესებულ მხარეებს ვაწვდით ინფორმაციას ჩვენი მისწრაფების, ინტერესების, საქმიანობის და მოღვაწეობის სფეროების შესახებ, რომლებიც შესაძლოა ჩვენთვის უცნობი და არასასურველი მიზნით, მათ შორის პროდუქციის თუ კომპანიის რეკლამირებისთვის, დაკოპირებული და გამოყენებული იქნეს სხვადასხვა ვებ-გვერდებსა თუ პლატფორმებზე.

სოციალური ქსელები აქტიურად ცდილობენ მომხმარებელთა პერსონალური მონაცემების დაცვას. მიუხედავად ამისა პროგრამული კოდის მოწყვლადობა არაერთმა შემთხვევამ დაადასტურა. მაგალითად, 2018 წელს Facebook-ის პროგრამულ უზრუნველყოფაში გაპარული ტექნიკური შეცდომის გამო 14 მილიონი მომხმარებლის სტატუსები რამდენიმე დღის მანძილზე საჯაროდ ხელმისაწვდომი გახდა. Instagram-ში არსებული ტექნიკური შეცდომის საშუალებით ჰაკერებმა 6 მილიონი მომხმარებლის, მათ შორის ცნობილი პირების, პერსონალური მონაცემები და მათი ფოტოები გაასაჯაროვეს. სოციალური ქსელების მმართველი კომპანიები ცდილობენ ამგვარი ტექნიკური პრობლემების აღმომჩენელ პირებთან თანამშრომლობით რისკების შემცირებას, თუმცა შეუძლებელია მომავალში მონაცემთა გაჟონვის გამორიცხვა. ლოკაციის – ადგილმდებარეობის მითითება Facebook სტატუსებში კიდევ ერთი საყურადღებო მოვლენაა. მიუხედავად იმის, რომ თქვენი ადგილმდებარეობის გასაჯაროება უწყინარ ამბად შეიძლება მიიჩნიოთ, ამგვარი ქმედება საკმაოდ სერიოზული რისკების მატარებელია. კრიმინალების მიერ მომხმარებლის შესახებ საჯაროდ ხელმისაწვდომი ადგილმდებარეობისა და სხვა მონაცემების შესწავლით მარტივად შეიძლება შედგეს მისი ყოველდღიური საქმიანობის და ადგილსამყოფელის ზუსტი სურათი და გამოყენებულ იქნეს მსხვერპლის სიცოცხლის, ჯანმრთელობის, ფინანსური, რეპუტაციული თუ სხვაგვარი ინტერესების საზიანოდ.

სოციალური ქსელების სტატუსებით, კომენტარებით, დამაინფიცირებელი ფაილებით, მესიჯებით, ვებგვერდებზე გადამისამართებით, თამაშებით, ბმულებით და მსგავსი მატარებლებით აქტიურად ვრცელდება მალვეარი, მავნე პროგრამული უზრუნველყოფა, ვირუსები. მომხმარებლები იმედოვნე-

ბენ, რომ გამომგზავნი არის სანდო წყარო და დაუფიქრებლად ხსნიან შეტყობინებებს, URL ბმულებს და შედეგად ინფიცირდებიან, ისევე როგორც ხელს უწყობენ მალვეარის ფართო გავრცელებას სხვა მომხმარებლებში.

მომხმარებელთა ანგარიშების გატეხვა და იმპერსონალიზაცია სოციალურ მედიასთან დაკავშირებული ფართოდ გავრცელებული საფრთხეებია. იდენტობის ქურდები ქმნიან

ყალბ ანგარიშებს, აკოპირებენ სხვა მომხმარებლების ფოტოებს, ამატებენ მათზე კომენტარებს, ცვლიან და აახლებენ ინფორმაციას, დებენ ახალ სტატუსებს, რომ მეტი დამაჯერებლობა შესძინონ საკუთარ ანგარიშს. ზოგიერთი მათგანი რამდენიმე სხვა ყალბ ანგარიშსაც აკეთებს – თითქოს ისინი მისი უახლოესი მეგობარი ან ახლობლები არიან, რომლებიც მოპარულ ფოტოებზე კომენტარებს უწერენ.

სოციალურ ქსელებს, მაგალითად Facebook-ს უსაფრთხოების პარამეტრების მართვის საკმაოდ ფართო სპექტრი გააჩნია. მომხმარებელს შეუძლია აკონტროლოს ვის და რა ინფორმაციაზე შეუძლია მონიშნოს, შეუძლია პროფილი დაიცვას უცნობი ადამიანების წვდომისგან და არ მისცეს მათ შემოსვლის შესაძლებლობა. ტვიტერზე პროფილის დახურვა და ნახვის შეზღუდვა შესაძლებელია, სანამ follower არ გახდება. google+-ზე შესაძლებელია მთელი რიგი კონფიგურაციების განხორციელება და წვდომის კონტროლი სხვადასხვა ინფორმაციულ აქტივზე.

სოციალური მედიის, მაგალითად Facebook-ზე არსებულ რომელიმე აპლიკაციაში, Facebook-ის ან google+-ის ანგარიშის გამოყენებით, თუნდაც ერთჯერადი შესვლისას შესაძლოა აპლიკაციებს წვდომა სამუდამოდ დარჩეთ, სანამ თქვენ მათ არ წაშლით.

ასევე ხშირია მესამე მხარის აპლიკაციების წვდომა სოციალური მედიის ანგარიშებზე, თუ მაგალითად Facebook-ის ანგარიშს მომხმარებელი იყენებს ამა თუ იმ აპლიკაციაში შესვლისთვის. ასეთ შემთხვევაში აპლიკაციებს ეძლევათ წვდომა მომხმარებლის და მისი მეგობრების მიერ Facebook-ზე განთავსებულ მონაცემებზე, რასაც სპამერები იყენებენ ანალიზის, მარკეტინგული ან/და სხვაგვარი მიზნით დამუშავებისთვის.

სოციალურ ქსელებთან დაკავშირებული საფრთხეების ასარიდებლად გამოიყენეთ შემდეგი კარგი პრაქტიკა:

თქვენი პესონალური ინფორმაცია ფასდაუდებელია, დაფიქრდით სანამ გაავრცელებთ მას!

მართეთ სოციალური ქსელის პარამეტრები. აკონტროლეთ პლატფორმის განახლებასთან ერთად ხომ არ იცვლება პარამეტრები.

ეცადეთ ყურადღება არ მიაქციოთ ‘ტროლებს’, არ უპასუხოთ, რადგან ეს სწორედ ის არის, რაც მათ უნდათ. ყველაზე სწორი ტაქტიკაა – დაბლოკოთ ისინი.

დაიმეგობრეთ მხოლოდ თქვენთვის ნაცნობი მომხმარებლები ან ისინი, ვისაც ავთენტიფიკაცია შეუძლია. ფრთხილად იყავით გაურკვეველი შინაარსის მქონე ანგარიშებთან, რომლებიც არ შეესაბამებიან სინამდვილეს.

არ გახსნათ უცხო პირებისგან მიღებული ბმულები და შეტყობინებები. ყურადღებით დააკვირდით გამოგზავნილ ბმულს და მის ადრესატს.

გაიაზრეთ რას ავრცელებთ საჯაროდ: საჯარო პოსტი ნიშნავს ყველასთვის, მთელი მსოფლიოსთვის ხელმისაწვდომობას.

დაფიქრდით, სანამ გააზიარებთ/გაავრცელებთ ინფორმაციას - ვინ არის სამიზნე აუდიტორია? გინდათ კი ეს ინფორმაცია თქვენი კონტროლის გარეთ მოხვდეს? მისი გავრცელება და ხანგრძლივობა უკონტროლო ხდება.

მართეთ მონიშვნები/თეგები. აკონტროლეთ, რომ თქვენი თანხმობის გარეშე არ განხორციელდეს თქვენი მონიშვნა ფოტოზე, ინფორმაციაზე.

არ გაუზიაროთ თქვენი ანგარიშის პარამეტრები არავის, ხშირად ცვალეთ ანგარიშის რეკვიზიტები, გამოიყენეთ უნიკალური და არა სხვა პლატფორმებზე უკვე გამოყენებული რეკვიზიტები.

მიიღეთ ყველა ზომა იმისთვის, რომ სოციალურ ქსელში განთავსებული პირადი მონაცემები არ იყოს ხელმისაწვდომი ნებისმიერი მომხმარებლისთვის. მაქსიმალურად დახურეთ პროფილი და იქ არსებული ინფორმაციის ნახვა შესაძლებელი გახადეთ მხოლოდ ახლობლებისთვის.

მოდული 11

ინფორმაციული წიგნიერება

ადამიანი კომუნიკაციისა და ინფორმაციის გავრცელებისთვის სხვადასხვა ხერხებსა და მექანიზმებს იყენებდა. ჯერ კიდევ დამწერლობის გავრცელებამდე, ადამიანები ერთმანეთს სხვადასხვა ფორმის მხატვრობით, ნიშნებითა და აუდიო-ვიზუალური გამოხატულებით ამყარებდნენ ურთიერთობას. გადაცემული ინფორმაციის სიზუსტე, სისრულე და სანდოობა ჯერ კიდევ საუკუნეების წინაც იწვევდა ეჭვებს და მათი შეფასება შესაბამისი სიფრთხილით ხდებოდა. ბეჭდური მედიის გამოჩენის კვალდაკვალ ყალბი ინფორმაციის გავრცელება გამარტივდა. ბევრი ჟურნალგაზეთის გამომცემლობა მიხვდა, რომ თუკი მათი პროდუქტის გაყიდვების გაზრდა სურდათ, მკითხველისთვის დამაინტრიგებელი, გასაოცარი, თუნდაც ყალბი სიახლეები უნდა დაეწერათ. ამ ყველაფერმა ბიძგი მისცა ინფორმაციულ პროპაგანდას. ბეჭდური მედიის გამოყენება მასებზე ზემოქმედების მოსახდენად აქტიურად ხორციელდებოდა პირველი და მეორე მსოფლიო ომის დროს. მხარეები მტრების ცუდად წარმოსაჩენად ინფორმაციას აზვიადებდნენ, ამახინჯებდნენ და საკუთარი ინტერესებისთვის ხელსაყრელად წარმოაჩენდნენ. მეოცე საუკუნიდან ინფორმაციით მანიპულირების კამპანიას უკვე სატელევიზიო არხიც შეუერთდა. შემდეგ გაჩნდა ინტერნეტი და ინფორმაციის მართვის პროცესები გართულდა – ნამდვილის და მოგონილის გარჩევა თითქმის შეუძლებელი გახდა.

ინტერნეტის მომხმარებელს საშუალება ეძლევა წეროს სტატუსები, შექმნას ბლოგები, შეტყობინებები და დაუსრულებლად გაავრცელოს ინფორმაცია. იგი ფასდაუდებელი რესურსია მიმდინარე და სანდო ინფორმაციის მისაღებად, რაც მნიშვნელოვანია სწავლის, მუშაობისა და გართობის პროცესში. ამასთანავე ინტერნეტი შეიძლება იყოს ინფორმაციული ქაოსის მომტანი, დეზინფორმაციის, ტყუილის პროპაგანდის, მავნე ინფორმაციისა და ყალბი სიახლეების წყარო. ინტერნეტში მასობრივად შევხვდებით ყალბი სიახლის ვებგვერდებს, სოციალური მედიის ყალბ ანგარიშებს, თაღლითურ რესურსებს, პროპაგანდისტულ ვებგვერდებს და ა.შ.

ინფორმაციული სივრცე წალეკილია „ყალბი სიახლეებით.“ როდესაც ინფორმაცია გარკვეულ სივრცეში ერთხელ მაინც მოხვდება, მისი უკან გამოხმობა უკვე ძალიან გვიანია, ინფორმაციის გავრცელება ვირუსულად ხდება. ინფორმაცია სწრაფად ვრცელდება და ბევრად უსწრებს მისი სანდოობის გადამოწმებისთვის საჭირო დროს. მარტივად ვიჯერებთ ინტერნეტში წაკითხულს, მოსმენილს, ნანახს. ინტერნეტმომხმარებლების უმეტესობას არ შეუძლია გაარჩიოს ერთმანეთისგან ყალბი და რეალური სიახლე.

„ყალბი სიახლე“ (Fake news) არის ინტერნეტში გავრცელებული სიახლე ან ამბავი, რომელიც არ შეესაბამება სიმართლეს. არსებობს ორი ტიპის ყალბი სიახლე: ა) გამიზნულად ვრცელდება ან იგზავნება, რათა ხალხმა დაიჯეროს რაღაც ან უბრალოდ ეწვიოს ვებგვერდს (ონლაინსივრცეში ბევრია მიზანმიმართული ტყუილი). ბ) ამბები, რომლებიც გარკვეულ სიმართლეს ასახავს, მაგრამ ყველა მონაცემი სანდო არ არის, რადგან ავტორი ინფორმაციის გამოქვეყნებამდე ყველა ფაქტს არ ამოწმებს ან უბრალოდ აზვიადებს. ყალბი სიახლეები სხვადასხვა მიზეზით იქმნება – უბრალოდ სახალისოდ, დაბნეულობის, ქაოსის გამოსაწვევად, მასებზე სხვადასხვა ნეგატიური ზეგავლენის მოსახდენად ან კომერციული მიზნით.

სოციალურმა მედიამ შეუძლებელი გახადა ინფორმაციული ნაკადების მართვა და გახდა ყველაზე მარტივი, ხელსაყრელი პლატფორმა ყალბი სიახლეების გასავრცელებლად. სიტყვის და აზრის გამოხატვის თავისუფლებით აღჭურვილი მომხმარებელი ხშირად წყაროს გადამოწმების გარეშე ქმნის/აზიარებს ონლაინ ინფორმაციულ რესურსებს და ამით მნიშვნელოვნად ზემოქმედებს სხვებზეც.

საყურადღებო ფენომენია ე.წ. „დიფ ფეიკი“ – ახალი დონის ტყუილი. არსებობს ტექნოლოგიური გადაწყვეტილება, რომლის გამოყენებითაც ხდება ადამიანის, მოვლენების ხელოვნურად დამუშავება/გაყალბება, ისეთი მდგომარეობის, სიტუაციისა და მოვლენის წარმოჩინება, რაც არასოდეს მომხდარა. ხელოვნური ინტელექტისა და ალგორითმების გამოყენებით არსებული/ნამდვილი აუდიო-ვიზუალური მასალიდან იქმნება სრულიად ახალი, ყალბი, არარეალური ფოტო-ვიდეო ნამუშევარი. უფრო მეტიც, დახვეწილი ხელოვნური ინტელექტის პროგრამებით შესაძლებელია არარსებული ადამიანების ფოტო-ვიდეო მასალების შექმნაც.

„დიფ ფეიკი“ ჩვეულებრივ გულისხმობს ისეთ აუდიო-ვიზუალურ ინფომაციას, რომელშიც ადამიანის, ხშირ შემთხვევაში საზოგადო მოღვაწის სახე და ხმა გაყალბებულია ხელოვნური ინტელექტის დახმარებით, ისე რომ შეცვლილი ვიდეო ავთენტურობას არ კარგავს. „დიფ ფეიკებს“ მიზანმიმართულად შეჰყავთ ადამიანები შეცდომაში. მაგალითად, გავრცელდება „დიფ ფეიკ“ ვიდეო პოლიტიკოსის მიმართვით, რაც მას რეალურად არ უთქვამს, ან „დიფ ფეიკ“ პორნოგრაფიული ვიდეო ცნობილი პიროვნებით, სინამდვილეში კი ეს სიმართლეს არ შეესაბამება. ახალი დონის ტყუილის ფართომასშტაბიანმა გავრცელებამ საგანგაშოდ დიდი გავლენა შეიძლება იქონიოს მასებზე მანიპულაციის, აზრის ჩამოყალიბების, დემოკრატიული პროცესებისა და არჩევნების სისტემებზე.

მედიასივრცე, ინტერნეტი, ონლაინპლატფორმები და სხვა კიბერრესურსები განსაკუთრებით ღირებული საშუალებაა დეზინფორმაციის გასავრცელებლად, საქართველოს წინააღმდეგ წარმოებული „ინფორმაციული ომის“ საწარმოებლად, იდეოლოგიურ-პროპაგანდისტული კამპანიებისთვის. რუსეთის ფედერაციიდან მომდინარე ინფორმაციული ომი, ანტიდასავლური ნარატივები განსაკუთრებული გამოწვევაა ქართული საზოგადოებისათვის და რუსეთის მხრიდან წარმოებული ჰიბრიდული ომის ნაწილს წარმოადგენს. დეზინფორმაციული კამპანიები რუსეთის მიერ საქართველოსა და ყოფილი საბჭოთა ქვეყნების წინააღმდეგ წარმოებული „რბილი ძალის“ შემადგენელი სტრატეგიული/ტაქტიკური, სისტემატური, რესურსებით კარგად უზრუნველყოფილი მასშტაბური ინსტრუმენტია. რუსეთის ფედერაცია საქართველოს წინააღმდეგ ინფორმაციულ ომს ეწევა, რისი ნათელი მაგალითებიცაა საქართველოს კრიტიკულ ინფორმაციულ სისტემებში უნებართვო შეღწევა, საიდუმლო/სენსიტიურ მონაცემებზე წვდომის მოპოვება, მათი წაშლა/დაზიანება და მოგვიანებით დეზინფორმაციის მიზნით გამოყენება.

2019 წლის ოქტომბერში საქართველოს პრეზიდენტის ადმინისტრაციის, სასამართლო სისტემის, სხვადასხვა მუნიციპალიტეტის საკრებულოების, სახელმწიფო, კომერციული და მედია ორგანიზაციების წინააღმდეგ განხორციელდა ფართომასშტაბიანი კიბერშეტევა. კიბერშეტევის შედეგად დაზიანდა ორგანიზაციების ტექნოლოგიური ინფრასტრუქტურა და მნიშვნელოვნად შეფერხდა მათი ფუნქციონირება, მათ შორის გარკვული დროით შეჩერდა სატელევიზიო ტრანსლირება. კიბერშეტევა მიზნად ისახავდა საქართველოს ეროვნული უსაფრთხოების ხელყოფას, საქართველოს მოსახლეობისათვის ზიანის მიყენებას და სამთავრობო სტრუქტურების, ასევე სხვადასხვა ორგანიზაციების ფუნქციონირების შეფერხებით და მოშლით საზოგადოებაში მღელვარების დათესვას. საქართველოს სამართალდამცავი ორგანოების მიერ ჩატარებული გამოძიებითა და საერთაშორისო პარტნიორებისგან მიღებული ინფორმაციით, აღნიშნული კიბერშეტევის უკან დგას რუსეთის ფედერაციის შეიარაღებული ძალების გენერალური შტაბის მთავარი სამმართველო („გრუ“). აშშ-მა, გაერთიანებულმა სამეფომ, ევროკავშირის არაერთმა წევრმა ქვეყანამ მყისიერად დაგმო მომხდარი კიბეროპერაცია, მის ორგანიზებასა და განხორციელებაში რუსეთის ფედერაცია დაადანაშაულა და აღნიშნული ოპერაციის მიზნად საქართველოში დემოკრატიული ინსტიტუტების ფუნქციონირების შეფერხება და საზოგადოებაში

დაუცველობის შეგრძნებისა და დესტაბილიზაციის შექმნა დაასახელა. პარტნიორებმა მოუწოდეს რუსეთს შეწყვიტოს მსგავსი კიბეროპერაციები და კიბერსივრცეში დაიცვას სახელმწიფოს პასუხისმგებლიანი ქცევის საერთაშორისო წესები. ამასთანავე, ევროატლანტიკურმა პარტნიორებმა გაანაცხადეს, რომ მხარს დაუჭერენ საქართველოს, როგორც კიბერუსაფრთხოების გაძლიერების, ასევე მავნე კიბერაქტორებთან ბრძოლის პროცესში.

რუსეთის მხრიდან წარმოებული დეზინფორმაციის ყველაზე ნათელი მაგალითია რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის წინააღმდეგ წარმოებული მასშტაბური ინფორმაციული და კიბერთავდასხმები, ანტივაქსერული პროპაგანდა, რაც მიზნად ისახავს საქართველოსა და მისი სტრატეგიული პარტნიორის - ამერიკის შეერთებული შტატების თანამშრომლობითი ურთიერთობისთვის ჩრდილის მიყენებას, მოსახლეობაში უნდობლობის გაჩენას. 2020 წლის სექტემბერში საქართველოს ოკუპირებული ტერიტორიების და დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს ინფორმაციულ სისტემაზე განხორციელებული კიბერშეტევის შედეგად სამინისტროსა და რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის მონაცემთა ბაზებში მოხდა უნებართვო შეღწევა და მათში დაცული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, შემდეგ კი სახეცვლილი - გაყალბებული ფორმით უცხოურ ვებგვერდებზე ხელმისაწვდომად განთავსება. აღნიშნული კიბერშეტევის მიზანი იყო საქართველოს ჯანდაცვის სისტემისთვის რეპუტაციული ზიანის მიყენება, ლუგარის ლაბორატორიის საქმიანობის კომპრომატირება, საქართველოს იმიჯის შელახვა მცდარი ინფორმაციის გავრცელებით.

საქართველოსთან მიმართებით რუსული დეზინფორმაციის ნარატივის მთავარი მოტივებია იდენტობა და ფასეულობები, საგარეო პოლიტიკური კურსი და ევროატლანტიკური მისწრაფებები. ნარატივები გაჯერებულია პრორუსული პროპაგანდით, რომელშიც აღმატებულად არის დახატული საბჭოთა წარსული და მართლმადიდებლური ქრისტიანობა.

ანტიდასავლური ნარატივების პარალელურად, საქართველოში, სოციალური ქსელებისა და ინფორმაციის მასობრივი გავრცელების სხვა საშუალებების გამოყენებით, გააქტიურდა კრემლის მიერ მართული მეზობელი სახელმწიფოების – აზერბაიჯანის, თურქეთისა და სომხეთის საწინააღმდეგო რიტორიკა (მაგ.: მთიანი ყარაბაღის კონფლიქტთან დაკავშირებით), რაც მიზნად ისახავს სამეზობლო-პარტნიორული ურთიერთობების დაზიანებას, ეთნიკური და რელიგიური შუღლის ჩამოგდებას, მეზობელი ქვეყნების იმიჯის დისკრედიტაციას.

კრემლის მომხრე პროპაგანდისტული მედიასაშუალებების კვალდაკვალ დეზინფორმაცია საქართველოში ადგილობრივი მედიის მიერ ქართულ ენაზე ვრცელდება, რადგანაც ხშირად ქართული წყაროები გადამოწმების გარეშე ან მიზანმიმართულად ავრცელებენ ცრუ ნარატივებს.

ვებგვერდებისა და მათზე განთავსებული ინფორმაციის სანდოობის ამოცნობის/გადამოწმების სხვადასხვა ხერხი არსებობს:

• ხშირ შემთხვევაში სენსაციური, შოკის მომგვრელი სათაური არის მანიშნებელი ცრუ ინფორმაციის. სენსაცია არის კარგი საშუალება მომხმარებლის მოსაზიდად. ასევე საყურადღებოა დაბალი ხარისხის ნიშნები, როგორებიცაა დიდი ასოებით დაწერილი სიტყვები, სათაურები შესამჩნევი გრამატიკული შეცდომებით, გამოკვეთილი მითითებები წყაროების გარეშე.

• ვებგვერდის წარმომავლობის გასარკვევად ეწვიეთ ვებ-გვერდის „ჩვენს შესახებ“ სექციას. გაარკვიეთ ვინ უჭერს მხარს და ვინ თანამშრომლობს მათთან. თუ მსგავს ინფორმაციას ვერ ნახავთ და ინფორმაციის მიღებამდე საიტი მოგთხოვთ რეგისტრაციას, უნდა დაფიქრდეთ რატომ არ არიან ისინი გამჭვირვალეები.

• გადაამოწმეთ სხვა სანდო საინფორმაციო საშუალებები თუ ავრცელებენ იგივე სიახლეს. თუ არა, ეს სულაც არ ნიშნავს, რომ სიახლე აუცილებლად არასანდოა, თუმცა საჭიროებს ღრმა კვლევას.

• სტატიის სანდოობაში დასარწმუნებლად სათაურებს ნუ დაუჯერებთ. მაცდური სათაურები გამოიყენება მომხმარებლის მიტყუების მიზნით. გაეცანით ვინ არის სტატიის ავტორი, რა წყაროებს იყენებს, რომელ ვებგვერდზეა განთავსებული. ინფორმაცია ნეიტრალური და პროფესიულად დამუშავებულია თუ მიკერძოებულია? ჰკითხეთ სა-

კუთარ თავს ვინ შეიძლება ისარგებლოს სტატიის გავრცელებით ან ვინ შეიძლება დაზარალდეს? რა არის სტატიის მიზანი - დისკრედიტაცია, სატირა? ფარული რეკლამა?

• მსოფლიო მასშტაბით იზრდება ელ. რესურსების რაოდენობა, რომლებიც სისტემატურად ეწევიან ფაქტების გადამოწმებასა და სიცრუის გამოვლენას. მოძიებული ინფორმაციის სანდოობის გადასამოწმებლად სხვადასხვა ვებ-გვერდი არსებობს, მაგალითად: FactCheckEU (https://factcheckeu.info/en/) – ევროპული პლატფორმა, პოლიტიკური პირების მიერ საჯარო გამოსვლებისას გაკეთებული განცხადებების, საარჩევნო მოწოდებების, სტატისტიკური თუ ხარისხობრივი მონაცემების გადამოწმება ხდება. ევროკავშირის ნებისმიერ მოქალაქეს უფლება აქვს კონკრეტული საკითხის/სტატიის სანდოობის შემოწმება მოითხოვოს ვებგვერდზე შესაბამისი განცხადების გაკეთებით, ხოლო ევროკავშირის მასშტაბით პროექტზე მომუშავე ჟურნალისტთა მთელი გუნდი იკვლევს საკითხს და საჯაროდ ხელმისაწვდომს ხდის საკითხის სანდოობის თუ სიყალბის შესახებ ინფორმაციას. Snopes: ამერიკული შესამოწმებელი ვებ-გვერდი – https://www.snopes.com/. მნიშვნელოვანია აგრეთვე EU East Stratcom-ის სამუშაო ჯგუფის მიერ შემუშავებული საქართველოზე გამიზნული დეზინფორმაციის მაგალითები – https://euvsdisinfo.eu/disinformation-cases/, ასევე ქართული რესურსები https://factcheck.ge/ka, https://www.mediachecker.ge/.

ინფორმაციული წიგნიერების კარგი პრაქტიკა:

ვებ-გვერდები, რომელთა მისამართები მთავრდება .gov (სამთავრობო), .edu (აკადემიური) ან .org (ასოციაციები, არასამთავრობო) არის უფრო სანდრო, ვიდრე .co-ით (სარეკლამო) დაბოლოებული.

სოციალურ სივრცეში გაზიარებამდე შეამოწმეთ ინტერნეტში მოძიებული ინფორმაცია (სიახლე, ვიდეოები, ფოტოები...) ფაქტების გადამოწმების სერვისების მეშვეობით, რათა თავიდან აიცილოთ დეზინფორმაციის გავრცელება.

გამოიყენე გვერდები, რომლებიც სპეციალურად ყალბი სიახლეების აღმოჩენისთვისაა გამიზნული.

საყურადღებოა ბმულების, ვებგვერდის უჩვეულო სახელები, მათ შორის ისეთები, რომლებიც ".com"-ზე მთავრდება – ისინი ხშირად ცდილობენ გაასაღონ თავი ლეგიტიმურ ვებგვერდებად.

ცნობიერების ამაღლება და საზოგადოებრივი მედეგობის გაძლიერება სისტემური ტრენინგებითა და საგანმანათლებო აქტივობებით.

მოდული 12

არჩევნები და კიბერუსაფრთხოება

ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების განვითარებასთან ერთად მსოფლიოში და მათ შორის საქართველოში დღის წესრიგში დადგა საარჩევნო პროცესში ინფორმაციული ტექნოლოგიების გამოყენების საჭიროება. დადებით გავლენებთან ერთად, გაიზარდა ტექნოლოგიებიდან მომდინარე საფრთხეები. ეს საფრთხეები არ უკავშირდება მხოლოდ ელექტრონულ არჩევნებს. ჩარევა/კიბერსაფრთხეების შექმნა, ინფორმაციით მანიპულირება საარჩევნო პროცესის ნებისმიერ ეტაპზე შეიძლება განხორციელდეს (წინასაარჩევნო, არჩევნების დღესა და შემდგომ პერიოდში). რისკები იქმნება როგორც ამომრჩეველთა განწყობებზე მანიპულირების გზით (დეზინფორმაციის გავრცელება, ყალბი ვებ-გვერდების, სოციალური ქსელების ანგარიშებისა და სხვა პლატფორმების გამოყენება მანიპულირებისათვის), სახელმწიფო ინსტიტუციების ვებგვერდების, სოციალური ქსელებისა, საარჩევნო ადმინისტრაციის ვებგვერდებში/პროგრამებში ჩარევის და მონაცემების/პერსონალური ინფორმაციების დაკარგვა/ცვლილების კუთხით.

კიბერსაფრთხის და კიბერდანაშაულის ჩადენა შეუძლია ნებისმიერ იურიდიულ თუ ფიზიკურ პირს და ის შეიძლება იყოს შიდა ან/და გარე აქტორი.

ჩარევის ობიექტი[6] შეიძლება გახდეს საარჩევნო პროცესში ჩართული ყველა აქტორი, ნებისმიერი სახელმწიფო ინსტიტუცია[7], არასამთავრობო, მედია ორგანიზაცია, პოლიტიკური პარტიები, მათი წარმომადგენლები და ლიდერები, ასევე ამომრჩეველი, რომლის ნების ჩამოყალიბებაზე გავლენას ახდენს ტრადიციული და ელექტრონული მედიით გავრცელებული ინფორმაცია.

ადგილობრივი თვითმმართველობების წარმომადგენლობითი და აღმასრულებელი ორგანოები თავიანთი კომპეტენციისა და საქმიანობიდან გამომდინარე ინახავენ და ამუშავებენ მოქალაქეების (მაგ: ჩართულობის მექანიზმების ამუშავებისთვის ამომრჩეველთა ერთიან სიებს) პერსონალურ ინფორმაციას. შესაბამისად, მნიშვნელოვანია მუნიციპალიტეტებს ჰქონდეთ მათ ხელთ არსებული პერსონალური და სხვა ტიპის ინფორმაციის დაცვის სტრატეგია და წესი, ასევე უნდა განსაზღვრონ ინფორმაციის დამუშავების ვადები, ფორმატი, დაშვების დონეები და ინფორმაციაზე წვდომაზე უფლებამოსილი პირები.

საარჩევნო პერიოდში აქტუალური ხდება საჯარო მოხელეების მიერ სოციალური ქსელების პერსონალური ანგარიშებიდან აგიტაციის შემცველი სტატუსების/მოწოდებების და სხვა აქტივობების განხორციელება. შესაბამისად, იზრდება რისკები მათ მიერ უკანონო აგიტაციის განხორციელების ან მათ წინააღმდეგ კიბერსაფრთხეების შექმნის კუთხით.

2016-2018 წლებში სოციალური ქსელების საშუალებით აქტუალური იყო „ტროლების“ და „ბოტების“ მიერ დეზინფორმაციის გავრცელება და საარჩევნო სუბიექტების თუ სადამკვირვებლო ორგანიზაციების დისკრედიტაცია. დეზინფორმაცია და ყალბი ინფორმაცია შემდგომაც არაერთხელ გავრცელდა და უფრო ფართო ხასიათი მიიღო.

მაგ: არასამთავრობო ორგანიზაცია სამართლიანი არჩევნების განცხადებით: „2017 წლის საპარლამენტო არჩევნების წინასაარჩევნო კამპანიაზე დაკვირვებამ ცხადყო, რომ Facebook-ი არამხოლოდ პოლიტიკური აქტორების მხრიდან საკუთარი პროგრამების და იდეების გასავრცელებლად ან დისკუსიისთვის, არამედ ცალკეული კანდიდატების დისკრედიტაციის მიზნითაც გამოიყენებოდა დეზინფორმაციისა და სხვადასხვა დამაზიანებელი ინფორმაციის გავრცელების გზით, რასაც ორგანიზებუ-

6 ამერიკის პრეზიდენტის არჩევნებში რუსეთის მიერ კიბერჩარევაზე იხილეთ ბმული:

7 საქართველოს კანონის ინფორმაციული უსაფრთხოების შესახებ მე-2 მუხლის ზ პუნქტის მიხედვით: კრიტიკული ინფორმაციული სისტემის სუბიექტი არის სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის.

ლი და მიზანმიმართული ხასიათი ჰქონდა. დაკვირვების პროცესში ასევე ცხადი გახდა, რომ სხვადასხვა საარჩევნო სუბიექტის დისკრედიტაციის გარდა, სოციალური მედია წარმატებით გამოიყენებოდა პოლიტიკურ ფინანსებსა და აგიტაციასთან დაკავშირებით საარჩევნო კანონმდებლობით დადგენილი აკრძალვების გვერდის ასავლელად".[8] აღნიშნული ნეგატიურ გავლენას ახდენს ამომრჩეველთა ნების ფორმირებაზე და მანიპულირების შესაძლებლობას იძლევა.

დეზინფორმაციის და ყალბი ინფორმაციის გავრცელება რამდენიმე გზით არის შესაძლებელი. მაგ: ამ მიზნით შექმნილი ყალბი ანგარიშებისა და ვებგვერდების საშუალებით, ან კიბერჩარევის და საჯარო მოხელეების ანგარიშების გამოყენებით. რაც კონკრეტული პირების დისკრედიტაციას, ასევე, უკანონო აგიტაციისთვის[9] პასუხისგებლობის დაკისრებას გამოიწვევს. ხოლო თუ ქმედება მოიცავს სისხლის სამართლის დანაშაულის ნიშნებს, პირს შესაძლოა დაეკისროს სისხლისსამართლებრივი პასუხისმგებლობაც.

ტექნოლოგიების განვითარებასთან ერთად სოციალურმა მედიამ არსებითი როლი შეიძინა ფართო მასებისთვის ინფორმაციის სწრაფად და ნაკლები დანახარჯებით გავრცელების კუთხით.

2016-2018 და 2020 წლების საარჩევნო ციკლს თუ გავაანალიზებთ, სოციალური მედია, განსაკუთრებით კი Facebook-ი წინასაარჩევნო კამპანიის/აგიტაციის მნიშვნელოვანი ინსტრუმენტი გახდა საქართველოშიც, განსაკუთრებით პანდემიის პირობებში.

სადამკვირვებლო ორგანიზაციების განცხადებით (GYLA, ISFED) საარჩევნო პერიოდში მთავარ გამოწვევას წარმოადგენდა:

√ საარჩევნო ადმინისტრაციის მიერ იმის არ აღიარება, რომ სოციალური მედია აგიტაციის/კამპანიის მნიშვნელოვანი ინსტრუმენტია (სოციალურ მედიაში უკანონო აგიტაციის/ამომრჩეველთა მოსყიდვის არაერთი ფაქტი დაფიქსირდა, რაც უგულვებელყოფილ იქნა, იმ მოტივით, რომ საარჩევნო კოდექსი არ არეგულირებს სოციალურ ქსელებში აგიტაცია/კამპანიას);

√ საჯარო მოხელეების მიერ პირადი გვერდებით კამპანიური ხასიათის სტატუსების გამოქვეყნება და საარჩევნო აგიტაცია/კამპანიის წარმოება;

√ ანონიმური გვერდების მიერ დასპონსორებული შინაარსის მეშვეობით წარმოებული ფართომასშტაბიანი დისკრედიტაციის კამპანია და ამ მიზნით დახარჯული თანხების გაუმჭვირვალობა, რომლის მონიტორინგის მექანიზმი აუდიტის სამსახურს არ გააჩნდა;

√ პროპაგანდისტული ნარატივების ანალიზი, რომელიც არა მხოლოდ შიდაპოლიტიკური პროცესების გამოძახილს, არამედ გეგმაზომიერ დეზინფორმაციულ და საინფორმაციო კამპანიას წარმოადგენდა, რომელიც მიმართული იყო ანტიდასავლური, ქსენოფობიური და ჰომოფობიური განწყობების გასაღვივებლად.

სოციალური მედიის აგიტაცია/კამპანიის ერთ-ერთ მნიშვნელოვან ინსტრუმენტად გამოყენება 2021 წლის ადგილობრივი თვითმმართველობის არჩევნებზე აქტუალური იქნება, მათ შორის COVID-19 გავრცელებისა და იმ შეზღუდვების ფონზე, რომელიც შესაძლებელია აუცილებელი გახდეს პანდემიის გამწვავების შემთხვევაში.

ვინაიდან სოციალურ მედიაში ვერ ხდება იმ სტანდარტების დაცვა, რომელიც მიუკერძოებლობისა და სამართლიანობის პრინციპების აღსრულებას ემსახურება საარჩევნო კამპანიის გაშუქებისას ჯერ კიდევ 2020 წლის არჩევნების წინასაარჩევნო პერიოდში არასამთავრობო ორგანიზაციებმა ოფიციალური წერილით მიმართეს Facebook-ის ადმინისტრაციას და მოითხოვეს აქტიური ქმედებები, რაც გულისხმობდა შემდეგს[10]:

√ რაც შეიძლება სწრაფი რეაგირება მოჰყოლოდა და ხელმისაწვდომი გამხდარიყო პოლიტიკური რეკლამების ბიბლიოთეკა საქართველოში, ისევე როგორც ეს მოხდა 2019 წელს უკრაინაში და ასევე ევროკავშირის ქვეყნებში ევროპარლამენტის არჩევნების წინ (შემდეგი ინფორმაციის გამჭვირვალობა: რეკლამის დამკვეთის/გადამხდელის ვინაობა, საკონტაქტო ინფორმაცია, თითოეული რეკლამისთვის დახარჯული თანხის ოდენობა და ვალუტა, რეკლამის განთავსების პერიოდი, პოსტის გავრცელების გეოგრაფიული არეალი და დემოგრაფიული დიაპაზონი).

8 სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოების ანგარიში.
იხილეთ ბმული:

9 საარჩევნო კოდექსით უკანონო აგიტაცია ეს არის, როდესაც პირები, რომელთაც სამუშაო საათების ან/და სამსახურებრივი ფუნქციების შესრულებისას აკრძალული აქვთ აგიტაციის (მხარდამჭერი ან საწინააღმდეგო ნებისმიერი საჯარო ქმედება, რომელიც ხელს უწყობს ან უშლის პირის არჩევას) განხორციელება.

10 იხილეთ განცხადების ბმული:

√ გაძლიერებულიყო ძალისხმევა საარჩევნო პერიოდში არაავთენტური კოორდინირებული ქცევის გამოსავლენად და მასში ჩართული ანგარიშების პლატფორმიდან დროულად წასაშლელად. ასევე, კოორდინირებული საეჭვო ქცევის გამოვლენისა და შესაბამისი ქსელების წაშლის შემდგომ, ამ ანგარიშების მიმდევრებისა და მომწონებლებისათვის Facebook-ს ეცნობებინა შეტყობინებით, რომ შესაბამისი ანგარიში წაიშალა კოორდინირებული საეჭვო ქცევის გამო.

√ Facebook-ს უნდა განევითარებინა და გაეღრმავებინა თანამშრომლობა შესაბამისი რეპუტაციის მქონე მიუკერძოებელ ადგილობრივ ორგანიზაციებთან, რომლებიც სოციალური მედიის მონიტორინგსა და ფაქტების გადამოწმებაზე მეთოდოლოგიურად მუშაობენ, მათ მიგნებებზე სწრაფი და ეფექტური რეაგირება უნდა მოეხდინა.

უნდა აეკრძალა პოლიტიკური რეკლამების მიკროტარგეტირება მომხმარებლის ქცევის მიხედვით.

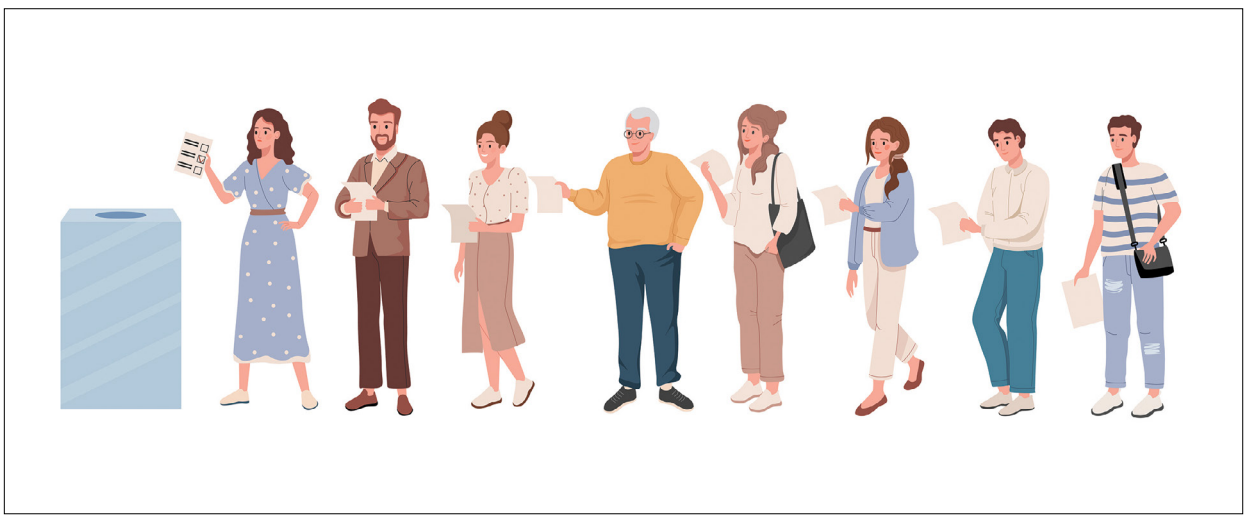
უნდა აეკრძალა უცხო ქვეყნის ტერიტორიიდან პოლიტიკური რეკლამის განთავსება.

Facebook-ს უნდა აემაღლებინა გვერდების გამჭვირვალობის სტანდარტი და გაეხსაჯაროვებინა გვერდების დადასტურებულ მფლობელთა შესახებ ინფორმაცია. ამასთან, კვლავ საჯარო უნდა გამხდარიყო Facebook-ის გვერდების ადმინისტრატორების რაოდენობისა და ლოკაციის, ასევე გვერდების სახელების ცვლილების შესახებ ინფორმაცია.
Facebook-ს უნდა შემოიღო ფაქტების გადამოწმების უფრო მკაფიო მონიშვნის შესაძლებლობა და ამისთვის თანამშრომლობა უნდა დაეწყო IFCN-ის მიერ აკრედიტირებულ ფაქტების გადამმოწმებელ ორგანიზაციებთან საქართველოში.
2020 წლის 15 ივლისს გამოგზავნილი პასუხით, ადმინისტრაციის მიერ აღინიშნა, რომ Facebook-ს აქვს მნიშვნელოვანი როლი და პასუხისმგებელია დაეხმაროს ადამიანებს მონაწილეობა მიიღონ დემოკრატიულ პროცესებში, უზრუნველყოს უსაფრთხო, დაცული და თავისუფალი არჩევნები. ადმინისტრაციამ დაადგინა გამჭვირვალობის სტანდარტები, რომელთა ფონზეც წარიმართა 2020 წლის საპარლამენტო არჩევნები. 2020 წლის აგვისტოდან Facebook-მა საქართველოში დაადგინა პოლიკური და საარჩევნო შინაარსის ინფორმაციის განთავსების სტანდარტები, კერძოდ:

- დაიწყო იმ პირების ავტორიზირება, რომლებიც პოლიტიკური და საარჩევნო ხასიათის შინაარსის აქტივობებს განახორციელებენ;

- დაიწყო დისქლეიმერის „Paid for by“ ასახვა დაფინანსებული ხასიათის აქტივობებზე, რომელიც უზრუნველყოფს ორგანიზაციების თუ ფიზიკური პირების საჯაროობას. ამ პირებმა Facebook-ის ადმინისტრაციას უნდა წარუდგინონ მისამართი, ტელეფონი, ელფოსტისა და ვებგვერდის მისამართები და ამ ინფორმაციას Facebook-ი 7 წლის მანძილზე შეინახავს;

- დაიწყო ფეიკ-ანგარიშების/ინფორმაციის იდენტიფიცირება და ამოღება.



საარჩევნო პროცესში ინფორმაციული და კიბერსაფრთხეების თავიდან ასარიდებლად

არ განახორციელოთ უკანონო აგიტაცია.

თქვენს სამსახურეობრივ ან პირად მოწყობილობებში უკანონო შეღწევის დაფიქსირების შემთხვევაში დაუყოვნებლივ მოახდინეთ რეაგირება.

მიიღეთ თქვენს ხელთ არსებული ყველა ზომა სამსახურებრივი და პერსონალური ინფორმაციის დაცვისათვის.

დაბეჭდილია საქართველოში
შპს არტსერვისის მიერ