რეკომენდაციები ადვოკატებისთვის კიბერ უსაფრთხოების მინიმალური სტანდარტების დაცვის თაობაზე

საქართველოს ადვოკატთა ასოციაცია

თინათინ ვირსალაძის ჩიხი I, № 1
დიღომი, თბილისი
(995 32) 298 78 78
info@gba.ge
www.gba.ge

ს.ს.ი.პ "საქართველოს ადვოკატთა ასოციაციის"
L.E.P.I. "GEORGIAN BAR ASSOCIATION"

რეკომენდაცია 1:

ყველა ანგარიშისა და მოწყობილობისთვის გამოიყენეთ გრძელი, უნიკალური პაროლი, უსაფრთხოების დამატებითი ელემენტით

გამოიყენეთ გრძელი პაროლი, რომელიც მარტივად დასამახსოვრებელია (მაგ. დიდი და პატარა ასოების გამოყენებით რაიმე ფრაზა სიმბოლოებისა და ციფრების დამატებით). კომპიუტერული პროგრამისთვის მსგავსი პაროლი ბევრად რთულად გამოსაცნობია, ვიდრე რაიმე მოკლე პაროლი. თუმცა, ყველაზე რთულად გამოსაცნობი პაროლიც კი უსარგებლოა, თუკი ის მაინც გახდება წარმატებული ჰაკერული თავდასხმის ობიექტი. მას შემდეგ, რაც ჰაკერები მოიპოვებენ კონკრეტული ანგარიშის პაროლს, მათი სამიზნე ხდება ანგარიშზე არსებული სხვა ინფორმაცია. აქედან გამომდინარე, ყველა ვებ-გვერდისთვის გამოიყენეთ უნიკალური პაროლი. რამდენიმე შრიანი თავდაცვის გამოყენება, რაც გულისხმობს უსაფრთხოების დამატებითი ფენების უზრუნველყოფას, მაგ. როგორიცაა ორფაქტორიანი ან სამფაქტორიანი ავტორიზაცია (ავთენტიფიკაცია), დამატებით ზრდის ანგარიშების უსაფრთხოებას. ორი ფაქტორის ავთენტიფიკაციის მეთოდები ეყრდნობა პაროლს და მეორე ფაქტორს, როგორიცაა თითის ანაბეჭდი ან სახის სკანირება. უსაფრთხოების დამატებითი ფენა კი შესაძლოა გამოიხატოს პაროლის შეყვანის შემდგომ ტელეფონის ან ელ-ფოსტის მეშვეობით დადასტურებით.

რეკომენდაცია 2:

გამოიყენეთ და განაახლეთ ანტი-მავნე პროგრამები, მაგ. ანტივირუსები

მავნე პროგრამებსა და ე.წ. ვირუსებს შეუძლიათ კომპიუტერული რესურსის სერიოზული დაზიანება, მასში არსებულ ინფორმაციაზე არაავტორიზებული წვდომის შესაძლებლობების შექმნა და კლიენტთათვის ადვოკატის სახელით არასათანადო შეტყობინებების გაგზავნაც კი. შესაბამისად, ანტი-ვირუსული პროგრამების გამოყენება რეკომენდებულია არა მხოლოდ ლეპტოპებისათვის, არამედ იმ ტელეფონებისა და პლანშეტებისთვისაც, რომლებშიც განთავსებულია მნიშვნელოვანი სამართლებრივი ინფორმაცია. ასევე, აუცილებელია ანტი-ვირუსული პროგრამების მუდმივი განახლება, რათა მოწყობილობები დაცული იყოს ახალი მავნე კოდებისა და ვირუსებისგან.

რეკომენდაცია 3:

გამოიყენეთ ინფორმაციის წაშლის უსაფრთხო მეთოდები

მონაცემები ინახება არა მარტო კომპიუტერებსა და ტელეფონებში, ასევე, სკანერებში, ქსეროქსებში და სხვ. ამასთანავე, მონაცემთა შენახვას უზრუნველყოფს როგორც მონაცემთა შესანახი გარე მოწყობილობები (მეხსიერების ბარათები, დისკები), ასევე მოწყობილობაში ჩაშენებული საშუალებები. მნიშვნელოვანია, ინფორმაცია დაცული იყოს მას შემდეგაც, რაც მოწყობილობები საქმიანობისთვის საჭიროდ აღარ მიიჩნევა. ამდენად, მისი წაშლა ან სხვაგვარი განადგურებაც უნდა მოხდეს უსაფრთხოდ. მონაცემთა უბრალოდ წაშლა ან დაფორმატება არ ნიშნავს, რომ მისი აღდგენა შეუძლებელია. ამდენად, ინფორმაციის მატარებელი მოწყობილობის გასხვისებამდე მასზე არსებულ ყველა მონაცემზე სხვა მონაცემი უნდა გადაეწეროს ან მსგავსი მოწყობილობა ფიზიკურად უნდა განადგურდეს. საოფისე ქაღალდის დამაქუცმაცებელთა უმეტესობას შეუძლია CD და DVD დისკების ფიზიკური განადგურება, თუმცა მყარი დისკებისა და SSD-ს განადგურება შეიძლება უფრო მეტ ხარჯთან იყოს დაკავშირებული. თუ მონაცემთა მატარებლები განადგურდა მესამე პირის მიერ ადვოკატის შენობის გარეთ, მიზანშეწონილია მესამე პირისგან დამადასტურებელი ცნობის მოთხოვნა, რომ ის ნამდვილად განადგურებულია.

რეკომენდაცია 4:

გამოიყენეთ კომუნიკაციის დაშიფვრის მეთოდი, როგორც დაცვის ერთ-ერთი საშუალება

მოწყობილობებზე სენსიტიური მონაცემების დაცვის ეფექტური გზა მათი დაშიფვრაა. დაშიფვრის მეთოდი მრავალფეროვანია. დღეისათვის ყველაზე უსაფრთხოა ორმხრივი დაშიფვრის სისტემა - E2EE. ეს უსაფრთხო კომუნიკაციის მეთოდია, რომელიც ხელს უშლის მესამე მხარეს, მოიპოვოს წვდომა მონაცემებზე, როცა ისინი ერთი სისტემიდან თუ მოწყობილობიდან მეორეს გადაეცემა. დაშიფვრის წყალობით, მოწყობილობაზე არსებული ყველა მონაცემი სრულად წაუკითხავი ხდება. შედეგად, ისინი დაცულია უცხო პირების წვდომისა და მანიპულაციებისგან. დაშიფვრა მონაცემებს გარდაქმნის რთულ კოდად, რომლის წაკითხვაც შეუძლიათ მხოლოდ იმ ადამიანებს, რომლებსაც აქვთ წვდომა პირად გასაღებზე (იგივე გაშიფვრის გასაღებზე) ან პაროლზე. თუ დაშიფრული მონაცემები ხელში ჩაუვარდებათ არაავტორიზებულ პირებს, ისინი ვერ შეძლებენ ვერც კოდის გაშიფვრას და ვერც მის შეცვლას.

ბევრ საკომუნიკაციო საშუალებას თავად აქვს გააქტიურებული დაშიფვრის ფუნქცია. პოპულარულ ელექტრონულ ფოსტებს (მაგ. Gmail, Outlook) ვებ-გვერდსა და აპლიკაციებში აქვთ ჩაშენებული დაშიფვრის ფუნქცია და მისი გამოყენება მარტივადაა შესაძლებელი აღნიშნული ფუნქციის გააქტიურების გზით. დაშიფვრის შესაძლებლობა ჩაშენებულია სმარტფონებსა და ლეპტოპებშიც, რაც იცავს მათზე განთავსებულ ინფორმაციას დაკარგვის შემთხვევაში. ამასთან ერთად, მოკლე ტექსტური შეტყობინებებით კომუნიკაციისას რეკომენდებულია მხოლოდ ისეთი აპლიკაციების გამოყენება, რომლებიც აღჭურვილია დაშიფვრის ფუნქციით.

ხშირად კომუნიკაციის ჩაწერა ხორციელდება სერვისის მომწოდებლების მეშვეობით. სერვისის პროვაიდერებს შესაძლოა ეკისრებოდეთ ვალდებულება, სამთავრობო უწყებებს მიანიჭონ წვდომა დაცულ საუბრებზე. თუმცა, იმგვარი სერვისები როგორებიცაა Skype, WhatsApp, Viber ან სხვა მსგავსი ინტერნეტთან წვდომაზე დაფუძნებული საშუალებები, რომლებიც კომუნიკაციის მიზნით იყენებენ ,,აპლიკაციის შიდა'' ზარებს, ევროკავშირის ყველა წევრ ქვეყანაში არ მიიჩნევა ელექტრონულ საკომუნიკაციო მომსახურებად და ამდენად, შედარებით უსაფრთხო საკომუნიკაციო საშუალებაა. ამასთან ერთად, მაშინ, როდესაც ამგვარი სერვისის მიმწოდებელს ქვეყანაში არ ჰყავს ტექნიკური პერსონალი, სამართალდამცავი ორგანოებისთვის რთულია ასეთ პროვაიდერებზე ზეწოლა, თუ მათ არ სურთ თანამშრომლობა, ვინაიდან სამართალდამცავებმა კოორდინაციისა და თანამშრომლობისთვის საერთაშორისო არხებს უნდა მიმართონ. შესაბამისად, ისეთი საკომუნიკაციო სერვისების გამოყენება, რომლებიც ფიზიკურად მხოლოდ სხვა იურისდიქციებში იმყოფებიან, შეიძლება იყოს ადვოკატების მიერ გამოყენებული დაცვის ღონისძიება ეროვნული უწყებების მხრიდან მიზანმიმართული მეთვალყურეობის წინააღმდეგ, ვინაიდან სამართალდამცავებს მათთან არ აკავშირებთ მჭიდრო თანამშრომლობა. ინტერნეტ წვდომაზე დაფუძნებული საკომუნიკაციო საშუალებების გამოყენება ასევე არის კომუნიკაციის მეტამონაცემების ჩაწერისგან თავდაცვის კარგი საშუალება.

რეკომენდაცია 5:

გამოიყენეთ ინტერნეტთან წვდომაზე დაფუძნებული საკომუნიკაციო საშუალებები

მობილური აპლიკაციების სწორად შერჩევისათვის მნიშვნელოვანია განხილულ იქნეს მათი ძირითადი მახასიათებლები.

Whatsapp ერთ-ერთი მთავარი ფუნქციაა ორმხრივი დაშიფვრა და მომხმარებლის ინტერნეტ პროვაიდერსა თუ მობილური სერვისების მომწოდებელ კომპანიას მიმოწერის წაკითხვის საშუალება არ აქვს.

Telegram და Facebook მესენჯერს არ აქვთ ორმხრივი დაშიფვრის ფუნქცია. ეს გულისხმობს იმას, რომ როდესაც კომუნიკაცია ხდება აღნიშნული აპლიკაციების საშუალებით, ის არ იქნება დაშიფრული და მესამე პირი, სერვერებზე წვდომის მოპოვების შემთხვევაში, თავისუფლად მოახერხებს მიმოწერის წაკითხვას.

Signal უსაფრთხოების სპეციალისტების მიერ ყველაზე უსაფრთხო მესენჯერად არის აღიარებული. ორმხრივი დაშიფვრა მისი მთავარი ფუნქციაა და სიგნალის სერვერებზე წვდომის მოპოვების შემთხვევაშიც კი, მიმოწერას გაურკვეველი სიმბოლოების ერთობლიობის სახე ექნება. ასევე, გარკვეული პერიოდის შემდეგ სიგნალზე არსებული მიმოწერა სერვერიდან ქრება.

Viber უსაფრთხოების ექსპერტების მიერ უსაფრთხო მესენჯერადაა აღიარებული. თუმცა, ციფრული უსაფრთხოების სპეციალისტების აზრით, უსაფრთხოების დაცვის და სანდოობის მიხედვით, უპირატესობა სიგნალს ენიჭება.

აღსანიშნავია, რომ უსაფრთხოებაზე ზრუნვა მუდმივი პროცესია. ანგარიშების უსაფრთხოება, გუგლისა და სოციალური ქსელების კონფიდენციალურობის პარამეტრები, ანტი-მავნე პროგრამები მუდმივად უნდა მოწმდებოდეს.

რეკომენდაცია 6:

შეარჩიეთ ინტერნეტთან წვდომაზე დაფუძნებული ყველაზე უსაფრთხო საკომუნიკაციო საშუალება

ვირტუალური კერძო ქსელი არის კავშირი მოწყობილობასა და ინტერნეტს შორის, რომელიც არის დაშიფრული. VPN მალავს თქვენს ნამდვილ IP მისამართს და მის ნაცვლად წარადგენს VPN სერვერის მისამართს. VPN ინტერნეტ სერვისის პროვაიდერის გამოყენების ნაცვლად მუშაობს მოწყობილობის ინტერნეტ კავშირის მარშრუტიზაციის გზით. VPN შუამავლის როლს ასრულებს კომპიუტერსა და ინტერნეტს შორის - მალავს თქვენს IP მისამართს. უფრო მეტიც, გაგზავნილი მონაცემები დაშიფრულია და თუ რაიმე გზით ხდება მათი ჩაჭრა, მაშინ მისი წაკითხვა შეუძლებელია ვიდრე ის დანიშნულების ადგილზე მივა. ონლაინ საძიებო სისტემებში (მაგ. Google-ში) შესაძლებელია უამრავი როგორც უფასო, ისე ფასიანი ვირტუალური კერძო ქსელის შეძენა და ინტერნეტ საქმიანობის მისი საშუალებით განხორციელება.

ზოგადად, უსადენო ინტერნეტი (WI-FI) არ არის შესაფერისი პროფესიონალური გამოყენებისთვის, რომელიც კონფიდენციალური ინფორმაციის მართვას მოიცავს, გარდა იმ შემთხვევისა, როდესაც დამატებით უზრუნველყოფილია დაცვა VPN-ის საშუალებით. მხოლოდ იმიტომ, რომ ინტერნეტზე წვდომა დაცულია პაროლით არ ნიშნავს, რომ ის უსაფრთხოა. თუ დაუდგენელი თავდამსხმელი გამოიყენებს იმავე ინტერნეტს, რომლითაც თქვენ სარგებლობთ და გამოიყენებს იმავე პაროლს, ვინაიდან პაროლი გაზიარებულია, ის ისევე შეძლებს ადვოკატის მონაცემების ნახვას, როგორც პაროლის გარეშე ინტერნეტის გამოყენებისას შეძლებდა. ამრიგად, ადვოკატმა თავი უნდა შეიკავოს VPN-ის გარეშე უსადენო ინტერნეტის გამოყენებისგან, თუ დარწმუნებული არ არის, რომ wi-fi-ს პაროლი შეიცვალა ბოლო ერთ ან ორ დღეში.

რეკომენდაცია 7:

ინტერნეტით სარგებლობისას გამოიყენეთ ვირტუალური კერძო ქსელი (VPN)