ციფრული უსაფრთხოების პრაქტიკული სახელმძღვანელო საჯარო მოხელეებისთვის


სსიპ სამსახურის მიური
საქართველო

ციფრული უსაფრთხოების პრაქტიკული სახელმძღვანელო საჯარო მოხელეებისთვის

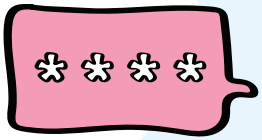
ილუსტრირებული გზამკვლევი

ავტორი: ნინო გამისონია

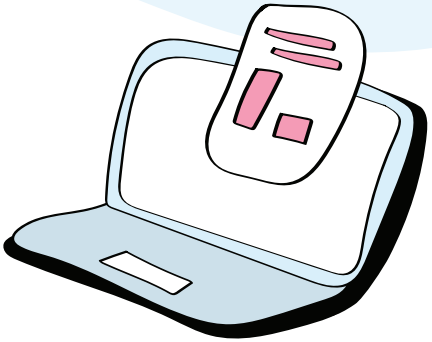
ილუსტრატორი: ნათია გოგრიჭიანი

დიზაინი და დაკაბადონება: გვანცა მახათაძე

სახელმძღვანელო მომზადებული და გამოცემულია საჯარო სამსახურის ბიუროს მიერ, გაეროს განვითარების პროგრამისა (UNDP) და შვედეთის მთავრობის ხელშეწყობით. გამოთქმული მოსაზრებები ავტორისეულია და შეიძლება არ ასახავდეს დონორი ორგანიზაციების თვალსაზრისს.

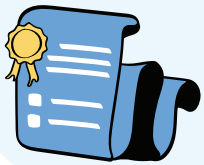


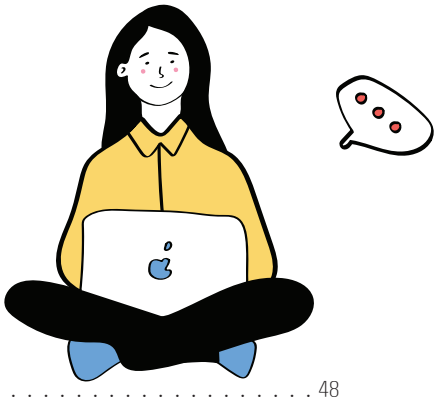
ციფრული უსაფრთხოების პრაქტიკული სახელმძღვანელო საჯარო მოხელეებისთვის

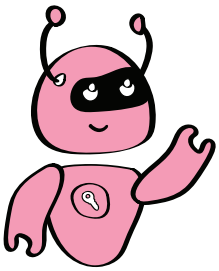


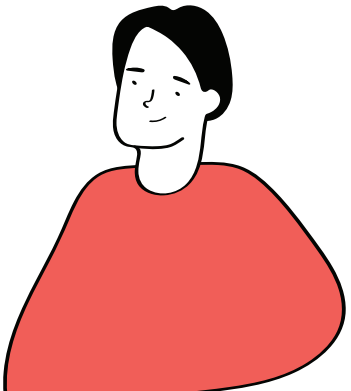
თბილისი 2022

სარჩევი









ტერმინთა განმარტება

„წესი 3-2-1“ – სარეზერვო ასლების შექმნის წესი

Google Authenticator – მობილური უსაფრთხოების აპლიკაცია, რომელიც დაფუძნებულია ორფაქტორიან ავტორიზაციაზე (2FA), რომელიც ეხმარება მომხმარებლის იდენტიფიკაციის გადამოწმებას ვებსაიტებზე და სერვისებზე წვდომის მინიჭებამდე

URL – ვებგვერდის მისამართი

IP მისამართი – უნიკალური ნომერი, მსგავსად სახლის ტელეფონის ან ელფოსტის მისამართისა, რომელიც დაკავშირებულია ყველა თქვენს მოქმედებასთან ინტერნეტში. ქსელის ნებისმიერი გამოყენებისას (საყიდლებისთვის, ელფოსტისთვის, ვიდეოების სანახავად), თქვენ აგზავნით მოთხოვნას შესაბამის დანიშნულების წერტილში, იქიდან კი საპასუხოდ იღებთ სასურველ ინფორმაციას. როგორ ხდება ეს? საქმე ისაა, რომ IP ნიშნავს ინტერნეტ ოქმს (Internet Protocol) და მოიცავს წინასწარ გაწერილ დებულებებსა და წესებს (იგივე ოქმი, დადგენილება) მონაცემების და მისამართებისა და ურთიერთკავშირისთვის. ამ ოქმით გაწერილი მითითებებით უნდა იხელმძღვანელოს ორივე მხარემ მონაცემების ურთიერთგაცვლისთვის

macOS – ოპერაციული სისტემა, რომელიც შემუშავებულია და რეალიზებულია Apple Inc.-ის მიერ 2001 წლიდან. ეს არის პირველადი ოპერაციული სისტემა Apple-ის Mac კომპიუტერებისთვის

Microsoft Store – ონლაინ მაღაზია მომხმარებლებისთვის, რომ შეიძინონ და ჩამოტვირთონ სხვადასხვა პროგრამები

ბინარული მონაცემები – მონაცემთა ტიპი, რომელიც წარმოდგენილია ან ნაჩვენებია ორობით რიცხვთა სისტემაში. ორობითი მონაცემები არის მონაცემთა ერთადერთი კატეგორია, რომლის უშუალო გაგება და შესრულება შესაძლებელია კომპიუტერის მიერ. ის რიცხობრივად წარმოდგენილია ნულებისა და ერთეულების კომბინაციით

განახლება (Update) – ახალი, გაუმჯობესებული ან დაფიქსირებული პროგრამული უზრუნველყოფა, რომელიც ცვლის იმავე პროგრამის ძველ ვერსიებს. განახლებები ხშირად უზრუნველყოფილია პროგრამული უზრუნველყოფის გამომცემლის მიერ დამატებითი გადასახადის გარეშე

გეოლოკაცია – მდებარეობის ტექნოლოგიების გამოყენება, როგორიცაა GPS ან IP მისამართები, რაც დაკავშირებულია ელექტრონული მოწყობილობების ადგილმდებარეობის დადგენასთან და თვალყურის დევნებასთან

დაშიფრული კომუნიკაცია – მეთოდი, რომლითაც ინფორმაცია გარდაიქმნება საიდუმლო კოდად, რომელიც მალავს გადაცემული ინფორმაციის ნამდვილ შინაარსს

დისკის დაშიფვრა – ტექნოლოგია, რომელიც იცავს ინფორმაციას წაუკითხავ კოდად გარდაქმნით, რომლის გაშიფვრა შეუძლებელია არაავტორიზებული ადამიანების მიერ

ვირტუალური კერძო ქსელი (VPN) – სერვისი, რომელიც დაგეხმარებათ, იყოთ კონფიდენციალური ონლაინ. ის აყალიბებს უსაფრთხო, დაშიფრულ კავშირს თქვენს კომპიუტერსა და ინტერნეტს შორის, უზრუნველყოფს კერძო გვირაბს თქვენი მონაცემებისა და კომუნიკაციებისთვის, სანამ იყენებთ საჯარო ქსელებს

კენსინგტონის კაბელი – უსაფრთხოების მოწყობილობა, რომლითაც კომპიუტერი შეგიძლიათ მიაბათ სტაციონარულ ობიექტზე, როგორიცაა მაგიდა. ის ჰგავს ველოსიპედის საკეტს, რომელიც უსაფრთხოდ ამაგრებს ველოსიპედს მოაჯირზე

მალვეარი – ყველა იმ პროგრამის სახელწოდება, რომელიც ცდილობს, მოიპოვოს უკანონო და არასანქცირებული გზების საშუალებით წვდომა მსხვერპლის კომპიუტერზე ან პროგრამა, რომელიც მიზანმიმართულად არის შექმნილი იმისათვის, რომ ავნოს მომხმარებლის კომპიუტერს ან მასში არსებულ ინფორმაციას, მომხმარებლისგან მალულად

ორნაბიჯიანი ავტორიზაცია (2FA) – უსაფრთხოების პროცესი, რომლის დროსაც მომხმარებლები უზრუნველყოფენ ორი განსხვავებული ავტორიზაციის ფაქტორს საკუთარი თავის შესამოწმებლად. 2FA დანერგილია როგორც მომხმარებლის პირადი მონაცემების, ისე რესურსების უკეთ დასაცავად, რომლებზეც მომხმარებელს შეუძლია წვდომა

რენსომვეარი (Ransomware) – კრიპტოვირუსოლოგიის მავნე პროგრამა, რომელიც მსხვერპლს პერსონალური მონაცემების გამოქვეყნებით ემუქრება ან სამუდამოდ დაბლოკავს მასზე წვდომას, თუ გამოსასყიდს არ გადაიხდი

უსაფრთხოების პატჩები – პროგრამული უზრუნველყოფა, რომელიც ასწორებს შეცდომებს კომპიუტერულ პროგრამულ კოდში. უსაფრთხოების პატჩები გამოშვებულია პროგრამული უზრუნველყოფის კომპანიების მიერ კომპანიის პროდუქტში აღმოჩენილი დაუცველობის აღმოსაფხვრელად.

პაროლების მენეჯერი – პროგრამა, რომელიც შექმნილია ონლაინ პირადი მონაცემების შესანახად და სამართავად. ჩვეულებრივ, ეს პაროლები ინახება დაშიფრულ მონაცემთა ბაზაში და ჩაკეტილია ძირითადი პაროლის უკან

ფაიარვოლი (firewall) – ქსელის უსაფრთხოების მოწყობილობა, რომელიც აკონტროლებს და ფილტრავს შემომავალ და გამავალ ქსელურ ტრაფიკს, ორგანიზაციის ადრე დადგენილი უსაფრთხოების პოლიტიკის საფუძველზე. firewall არსებითად არის ბარიერი, რომელიც დგას კერძო შიდა ქსელსა და საჯარო ინტერნეტს შორის

ფიშინგი – (ინგლ. phishing: fishing – თევზაობა + phreaching – სატელეფონო თაღლითობა) — ინტერნეტ-თაღლითობის და კიბერ დანაშაულებრივი ფორმა, ელფოსტის ან სხვაგვარი შეტყობინებების გაგზავნა ცნობილი რეალური ორგანიზაციის სახელით ან ლოგოთი

ქუქის (Cookies) – ვებგვერდის მონაცემების ნაწილი, რომელიც ინახება თქვენს მოწყობილობაზე, რომელიც ვებგვერდს შეუძლია მოგვიანებით მოიძიოს. ქუქი-ფაილები გამოიყენება სერვერისთვის სათქმელად, რომ მომხმარებელი დაბრუნდა კონკრეტულ ვებგვერდზე

შესავალი

21-ე საუკუნეში ციფრული შესაძლებლობების გამოყენება მთელ მსოფლიოში უფრო და უფრო ფართო მასშტაბებს იძენს. ახალ ტექნოლოგიებს ჩვენი შესაძლებლობებისა და კეთილდღეობის გასაძლიერებლად, ასევე, ჩვენს ყოველდღიურ ცხოვრებასა თუ სამსახურებრივ საქმიანობაში ვიყენებთ. თუმცა, მათი გამოყენებისას ადამიანები მნიშვნელოვანი ციფრული რისკების წინაშე დგებიან – შეიძლება, მათ საქმიანობას თუ ყოველდღიურ ცხოვრებას კიბერკრიმინალებმა შეუქმნან საფრთხე და თავს დაესხან დაუცველ მოწყობილობებსა და ქსელებს. შესაძლოა, ამ თავდასხმებმა მძიმე შედეგებამდე მიგვიყვანოს, დაწყებული ინდივიდუალური ზიანიდან (მაგ. შანტაჟი), მთელი სამუშაო სივრცისა და საჯარო სამსახურში არსებული ინფორმაციის დაზიანებამდე.

„ციფრული უსაფრთხოების პრაქტიკული სახელმძღვანელო საჯარო მოხელეებისთვის“ დაგეხმარებათ, გააცნობიეროთ თქვენი რეალური ციფრული სისუსტეები და გააძლიეროთ თქვენი ციფრული ცოდნა.

„ციფრული უსაფრთხოება“ ზოგადი ტერმინია და ერთდროულად ბევრ საკითხს მოიცავს. ციფრული უსაფრთხოების მიზანია ჩვენი სამსახურის, საკუთარი თავისა და სხვების დაცვა ციფრულ მოწყობილობებთან დაკავშირებისას. „ციფრული უსაფრთხოების პრაქტიკული სახელმძღვანელო საჯარო მოხელეებისთვის“ დაგეხმარებათ, გაიაზროთ, შეისწავლოთ და მართოთ საკუთარი ციფრული უსაფრთხოება. მას 6 თემატურ მიმართულებად ვანაწილებთ: ციფრული რისკები, პაროლები, მოწყობილობები, მონაცემები, ციფრული კომუნიკაცია, ციფრული იდენტობა.

თავი 1. ციფრული რისკები

ინტერნეტთან დაკავშირებულ ნებისმიერ აქტივობას თან ახლავს დაუცველობა. შესაძლებელია მონაცემების მოპარვა, კომუნიკაციების ჩაჭრა, თანამშრომლების მხრიდან ლეპტოპებისა და ტელეფონების შემთხვევით დაკარგვა, თავდამსხმელების მიერ ქსელების, ელფოსტისა და სოციალური მედიის ანგარიშების გატეხვა. ნებისმიერმა ასეთმა ინციდენტმა შეიძლება გამოიწვიოს მნიშვნელოვანი ფინანსური ზარალი, სამუშაოს შეფერხება და ზიანი მიაყენოს თქვენი სამსახურის რეპუტაციას.

საჯარო მოხელეებისთვის ციფრული რისკები სხვადასხვანაირია. მაგალითად, ბევრს თქვენი ონლაინ მოტყუება უნდა იმისთვის, რომ საჯარო უწყებების სისტემებში შეაღწიოს, თქვენს მოწყობილობებში არსებული მონაცემები მოიპაროს, დააზიანოს საჯარო სამსახურის კუთვნილი მოწყობილობები, სამსახურის ქსელში ვირუსი გაავრცელოს და ა.შ. ეს შეიძლება გააკეთონ სოციალური ინჟინერიის (ანუ ფსიქოლოგიური მანიპულაციის), ფიშინგისა და მალვეარების (ვირუსი) მეშვეობით. მართალია, ამ რისკების ბოლომდე აღმოფხვრა არ გამოვა, მაგრამ მათი საგრძნობლად შემცირება შესაძლებელია, თუკი ციფრულ ჰიგიენასა და საღ აზრს მოვუხმობთ.

რა ციფრული რისკები არსებობს

მოწყობილობების რისკი – მოწყობილობები, რომლებსაც ახლა იყენებთ, შესაძლოა, რამდენიმე წელიწადში მოძველდეს. მიიღეთ კარგად ინფორმირებული გადაწყვეტილება, როდესაც ირჩევთ მოწყობილობას თქვენი სამსახურისთვის. ასევე, დარწმუნდით, რომ საჯარო სამსახურში გამოყენებული მოწყობილობები სათანადოდ იყოს დაცული, რათა მათზე კიბერთავდასხმა რ მოხდეს.

მონაცემთა რისკი – როგორც მოგეხსენებათ, საჯარო უწყებების მოწყობილობებში არსებული მონაცემები განიხილება, როგორც ერთ-ერთი მთავარი სამიზნე თავდამსხმელებისთვის. მონაცემთა რისკი, მათ შორის, საჯარო უწყებაში შენახული სენსიტიური მონაცემები, ასევე, მომხმარებლების მონაცემები, შესაძლებელია, ბოროტად გამოიყენონ – გაასხვისონ, გაყიდონ ან დაშიფრონ შემდგომში გამოსასყიდის მოთხოვნის მიზნით.

რეპუტაციული რისკი – საჯარო მოხელის ანგარიშის გატეხით, შესაძლოა, ბოროტმოქმედმა მისი სახელით ისარგებლოს და მოქალაქეებს მოსთხოვოს თანხა ან კონკრეტული ინფორმაცია მესამე პირზე, მოიპოვოს არასაჯარო ინფორმაცია, გამოიყენოს საჯარო მოხელის სახელი და ელექტრონული ფოსტა ფიშინგ შეტევისთვის, მისწეროს სხვა თანამშრომლებს ან მოქალაქეებს უხამსი შინაარსის წერილები და ა.შ. ამით კონკრეტულ უწყებას და ზოგადად საჯარო სამსახურს რეპუტაციული ზიანი მიადგება და რეაბილიტაციას შეიძლება დიდი დროც დასჭირდეს.

კონფიდენციალურობის რისკი – თუ თქვენი სამსახური ინახავს პერსონალურ საიდენტიფიკაციო ინფორმაციას, თქვენ უნდა გქონდეთ შემუშავებული პროცესი, რომელიც აღწერს, ვინ ამუშავებს, ინახავს და იცავს თქვენი მომხმარებლებისგან შეგროვებულ პერსონალურ მონაცემებს. თქვენ შეგიძლიათ, გადახედოთ შესაბამის საკანონმდებლო ჩარჩოს, რომელიც არეგულირებს, თუ როგორ უნდა მოიქცეს საჯარო მოხელე პერსონალური მონაცემის დამუშავებისას.

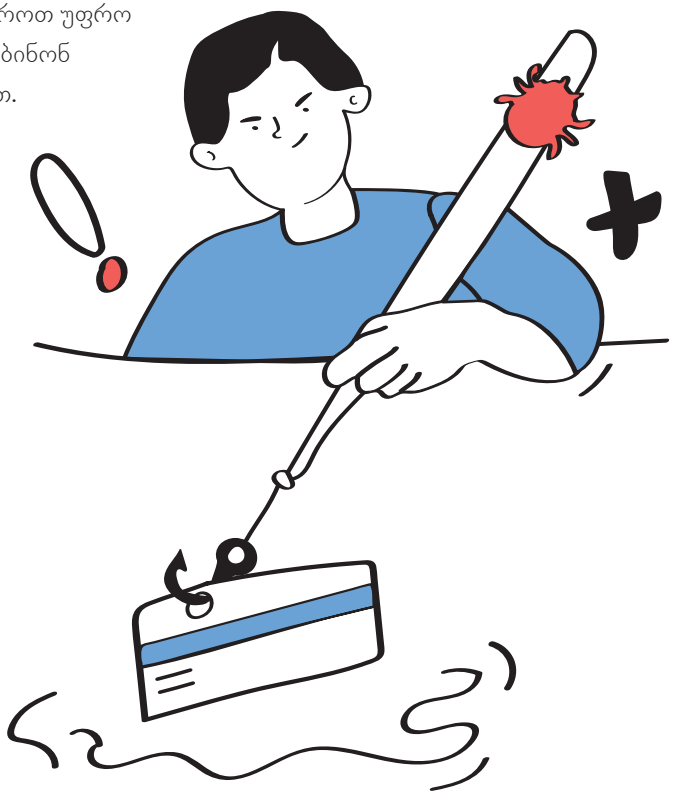
სოციალური ქსელების რისკი – თუ საჯარო უწყებას გააჩნია გვერდი სოციალურ მედიაში, აუცილებლად დარწმუნდით, რომ თანამშრომელს, რომელიც გვერდს მართვას, გამართული აქვს მოწყობილობა და ის სუფთაა ვირუსებისგან, ასევე, დაცულია მისი პირადი ანგარიში გარე თავდასხმისგან. გვერდის ადმინისტრატორის ანგარიშის გატეხვის შემთხვევაში, თავდამსხმელი ასევე მოიპოვებს უფლებას, წაშალოს საჯარო უწყების სახელით არსებული გვერდი, მიითვისოს ან სახელი გადაარქვას ამ გვერდს, ან არასაჯარო, სენსიტიური ან უხამსი შინაარსის ინფორმაცია გამოაქვეყნოს საჯარო უწყების სახელით.

როგორ ამოვიცნოთ ფიშინგ შეტევები

ყველაზე გავრცელებული ონლაინ საფრთხეები, რომლებსაც ყოველდღიურად ასობით მილიონი მომხმარებელი აწყდება, დაკავშირებულია სოციალური ინჟინერიის სქემებთან. თავისი არსით სოციალური ინჟინერია არის ხალხის მოტყუება სენსიტიური ინფორმაციის მოსაპოვებლად ან უსაფრთხოების ნორმალური პროცედურების დასარღვევად.

რა არის ფიშინგი?

ფიშინგ-შეტევები სოციალური ინჟინერიის ყველაზე გავრცელებულ სქემებს შორისაა. ბოროტმოქმედები იყენებენ ელფოსტას, სოციალურ მედიას და მოკლე ტექსტურ შეტყობინებებს (SMS), რათა გამოგტყუონ ინფორმაცია, რომელიც შეიძლება დაეხმაროთ უფრო დიდი დანაშაულის ჩადენაში. ასევე, მათი მიზანია, დაგაყენებინონ მავნე პროგრამა ბმულზე დაწკაპუნებით ან დანართის გახსნით.



ფიშინგ-შეტევების უმეტესობა ხორციელდება შეტყობინებების მასობრივი დაგზავნით. ისინი სანდო ჩანს და მოდის წყაროდან, რომელსაც ჩვეულებრივ ენდობით (მაგ. სახელმწიფო სააგენტო, ბანკი ან სოციალური მედიის სერვისი). მაგრამ, ასევე არსებობს ისეთი ფიშინგ-შეტევები, რომლებიც მიმართულია კონკრეტულ ინდივიდებზე ან ჯგუფებზე და თაღლითები მუდმივად იფიქრებენ ინოვაციებს და ცვლიან თავიანთ ინსტრუმენტებსა და მეთოდებს.

ფიშინგ-შეტევების სახეობები

ფიშინგ-შეტევების ყველაზე გავრცელებული სახეობებია:

- **„გამჭოლი ფიშინგი“ (Spear phishing)** – ფიშინგ-თავდასხმის სახეობა, რომლის დროსაც თაღლითი მიზანში იღებს კონკრეტულ ადამიანს, რათა მოატყუოს ის ელ-

ფოსტის, სოციალური მედიის, მოკლე ტექსტური შეტყობინების ან ჩეტ-შეტყობინებების საშუალებით. წერილები დამაჯერებლად გამოიყურება და თითქოს იღებთ მათგან, ვისაც იცნობთ – მაგ. კოლეგისგან ან მეგობრისგან.

- **„თავდასხმები ვეშაპზე“ (Whaling attack)** – არის გამჭოლი ფიშინგ-თავდასხმები, რომლებიც მიზნად ისახავენ „დიდი თევზის დაჭერას“. მათი სამიზნე არიან სამსახურების ხელმძღვანელები. ბოროტმოქმედები ელფოსტით აგზავნიან თაღლითურ შეტყობინებებს, რომლებიც ჰგავს მთავრობის ოფიციალური პირის, პარტნიორების ან დონორი ორგანიზაციების მიერ გამოგზავნილს.
- **SMiShing** თავდასხმები მოიცავს მოკლე ტექსტურ შეტყობინებებს (SMS) (ტექსტებს). თაღლითებმა შეიძლება თქვენს ნაცნობებად გაასაღონ თავი, რათა მოგთხოვონ ფული ან პირადი ინფორმაცია. ყველაზე ხშირად, ამ თავდასხმების ორგანიზატორები თავს ასაღებენ იმ სერვისების წარმომადგენლებად, რომლებსაც იყენებთ (მაგ. საკურიერო კომპანია, ონლაინ სავაჭრო პლატფორმა, ბანკი). ისინი გთხოვენ თანხის გადახდას ან გთავაზობენ სხვადასხვა სერვისების განახლებას.
- **Vishing** თავდასხმები მოიცავს ხმოვანი ზარების გამოყენებას. თაღლითები, რომლებიც ახორციელებენ ასეთ თავდასხმებს, ხშირად წარადგენენ თავს სამთავრობო უწყებების თანამშრომლებად. ისინი, როგორც წესი, იყენებენ მუქარას და საუბრის დამაჯერებელ მანერას, რათა მსხვერპლებმა იგრძნონ, რომ სხვა გზა არ აქვთ, გარდა იმისა, რომ მოთხოვნილი ინფორმაცია მიაწოდონ თაღლითებს.

ფიშერები ანუ ფიშინგ-თაღლითები უმიზნებენ თქვენს ემოციებს

ფიშინგ-თავდასხმების უმეტესობას აერთიანებს ის, რომ ისინი ცდილობენ, გამოიყენონ ძლიერი ადამიანური ემოციები. მათ შორის:

- **სიხარბე:** თავდამსხმელები, როგორც წესი, გთავაზობენ ფინანსურ ჯილდოს ან სხვაგვარ წახალისებას, თუ უბრალოდ დააწკაპუნებთ ბმულზე, გახსნით დანართს ან შეავსებთ ფორმას.
- **გადაუდებლობა:** თავდამსხმელები ქმნიან გადაუდებელი საქმის შეგრძნებას, მოქმედების მჭიდრო ვადით.
- **ცნობისმოყვარეობა:** თავდამსხმელები ატყუებენ მსხვერპლს და უნიკალური და საინტერესო შინაარსის დაპირებით, ცდილობენ აიძულონ ადამიანი, დააწკაპუნოს ბმულზე.
- **შიში:** თავდამსხმელები „აფრთხილებენ“ მსხვერპლს ნეგატიური შედეგების შესახებ, იმ შემთხვევაში, თუ არ გააკეთებს იმას, რასაც სთხოვენ.

ფიშინგის ელექტრონული ფოსტის ამოცნობა

ფიშინგის ტაქტიკა მუდმივად ვითარდება. ფიშერები თქვენს მოსატყუებლად ხშირად ბაძავენ სხვებს და იყენებენ ნამდვილი ორგანიზაციების ლოგოებს. თუმცა, ბევრ ფიშინგ-წერილს აქვს ქვემოთ ჩამოთვლილი ერთი ან რამდენიმე საერთო მახასიათებელი, რაც დაგეხმარებათ ასეთი თავდასხმების აღმოჩენაში:

- **ელფოსტის ყალბი მისამართები**, რომლებიც თქვენს მოსატყუებლადაა შექმნილი, გამოიყურება, როგორც რეალური მისამართები. მაგალითად, თავდამსხმელებმა შეიძლება მოგაჩვენონ თავი, რომ Amazon-ის წარმომადგენლები არიან, რათა მოიპაროონ თქვენი მონაცემები. ამისთვის გთხოვენ მათ „განახლებას“ ან „დადასტურებას“. უნდა დაეჭვდეთ, როდესაც მეილს იღებთ მაგ. ასეთი მისამართიდან: @amazonheadoffice.com ან @amazzon.com – @amazon.com-ის ნაცვლად. ასევე, გასათვალისწინებელია, რომ არც ერთი ნამდვილი და დიდი ორგანიზაცია წერილებს არ გამოგიგზავნით @gmail.com-დან, @mail.ru-დან ან სხვა ელექტრონული ფოსტის პლატფორმიდან, რომელიც შექმნილია ფართო საზოგადოებისთვის.
- **ჩაშენებული ბმულები**, რომლებიც მათზე დაწკაპუნებისას გადაგიყვანთ მავნე პროგრამით დაინფიცირებულ ყალბ ვებსაიტებზე. არასოდეს დააწკაპუნოთ ბმულებზე, სანამ არ შეამოწმებთ, სად გადაჰყავხართ მას. შეგიძლიათ იხილოთ ვებსაიტის სრული მისამართი, თუ დაჭერის გარეშე, უბრალოდ გადაატარებთ თქვენს მაუსს ბმულზე. სანამ დააწკაპუნებთ ბმულზე, რომელიც ოდნავ მაინც მიგაჩნიათ საეჭვოდ, დაასკანერეთ ბმულების სკანერით. მაგალითად, Norton Safe Web-ით.

  დაასკანერე Norton Safe Web

  განსაკუთრებული სიფრთხილე გამოიჩინეთ, როდესაც საქმე გაქვთ შემოკლებულ URL ბმულებთან. იმისათვის, რომ გადაამოწმოთ შემოკლებული URL ბმულის მიღმა არსებული სრული ბმული, გამოიყენეთ ისეთი უფასო ონლაინ სერვისი, როგორიცაა UnshortenIt).

  დაასკანერე UnshortenIt

- **დანართები** ანუ მიმაგრებული ფაილები, რომლებიც გახსნისთანავე აინფიცირებენ თქვენს მოწყობილობებს მავნე პროგრამით. ეს არის ციფრული უსაფრთხოების ერთ-ერთი ყველაზე ფუნდამენტური წესი – არასოდეს გახსნათ დანართები ანუ მიმაგრებული ფაილები, რომლებიც მიიღეთ იმ გამომგზავნებისგან, ვისაც არ იცნობთ ან სრულად არ ენდობით. ასევე, ნამდვილი ორგანიზაციები არასოდეს გამოგიგზავნიან დანართებს, თუ კონკრეტულად არ სთხოვთ მათ რაიმეს გაგზავნას.

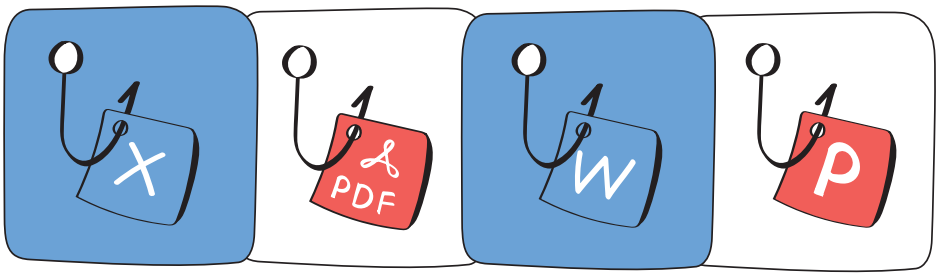
- **ცუდი გრამატიკა ან საუბრის უცნაური მანერა.** თაღლითები, რომლებიც იყენებენ წერილების მასობრივ დაგზავნას ფიშინგ-თავდასხმების განსახორციელებლად, ხშირად მიზნად ისახავენ ადამიანების მოტყუებას ათეულობით სხვადასხვა ქვეყანაში. იმის ნაცვლად, რომ თანხა ჩადონ შეტყობინების გადათარგმნაში და ადგილობრივ აუდიტორიაზე მის მორგებაში, ისინი იყენებენ ონლაინ თარგმანის უფასო სერვისებს. შედეგად, ფიშინგის მეილებში იყენებენ არაბუნებრივ ან აშკარად უცნაურ ენას. ხშირია გრამატიკული შეცდომები.
- **ზოგადი მისალმება** თქვენი სახელის ნაცვლად. როდესაც წერილი ზოგადი მისალმებით იწყება – „ძვირფასო მომხმარებელო“, „ძვირფასო ანგარიშის მფლობელო“ ან „ჩვენო ძვირფასო წევრო“ – ამან აუცილებლად უნდა დაგაეჭვოთ. ნამდვილმა ორგანიზაციებმა, რომლებიც გიკავშირდებიან, ხშირ შემთხვევაში, იციან თქვენი სახელი.

როგორ არ წამოვეგოთ ფიშინგზე

ფიშინგ-თაღლითობა ისეთივე ძველია, როგორც თავად ინტერნეტი და მისი გაქრობა ნაკლებად სავარაუდოა. საბედნიეროდ, როგორც წესი, ფიშინგის თავიდან აცილება ადვილია, თუ იყენებთ ციფრული უსაფრთხოების ძირითად წესებს. მიჰყევით ამ ძირითად ინსტრუქციებს, რათა იყოთ დაცული.

- **იყავით სკეპტიკოსი**

ყოველთვის გახსოვდეთ, როდესაც ინტერნეტში გთავაზობენ რაღაცას, რაც უბრალოდ მეტისმეტად კარგია, დიდი შანსია, გატყუებდნენ. თაღლითებს და კრიმინალებს კარგად ეხერხებათ ჩვენი ემოციებით, განსაკუთრებით კი სიხარბითა და ცნობისმოყვარეობით მანიპულირება. „გსურთ უახლესი iPhone სულ რაღაც 20 დოლარად?“, „გსურთ, გამოიმუშაოთ ბევრი ფული ყველა იმ პროდუქტის გასინჯვით, რომელსაც



კომპანიები უფასოდ გამოგიგზავნიან?“, „გსურთ, გაიგოთ, თქვენს რომელ კლასელს ან თანამშრომელს უყვარხათ ფარულად?“ ჯილდოების მისაღებად მხოლოდ ბმულზე დაწკაპუნებას, მიმაგრებული ფაილის გახსნას ან ფორმის შევსებას გთხოვენ. ნუ წამოეგებით ამ მახეს. თავი არ მოატყუებინოთ.

- **უფრთხილდით დანართებს ანუ მიმაგრებულ ფაილებს**

ეს არის ციფრული უსაფრთხოების ერთ-ერთი ყველაზე ფუნდამენტური წესი – არასოდეს ჩამოტვირთოთ და არ გახსნათ დანართები, რომლებსაც გიგზავნიან ელფოსტაზე, მესენჯერებში ან მოკლე ტექსტური შეტყობინების სახით ის ადამიანები, რომლებსაც არ იცნობთ ან სრულად არ ენდობით. თაღლითებსა და კრიმინალებს განსაკუთრებით უყვართ Word-ის, Excel-ის, PowerPoint-ის და PDF-ის დანართები. თუ ელფოსტა ან სხვა ტიპის შეტყობინება თქვენთვის უცნაურად ან საეჭვოდ გამოიყურება, საუკეთესო გზა თავის დასაცავად მისი დაუყოვნებლივ წაშლაა.

ასევე, გახსოვდეთ, მათაც კი, ვისაც ვენდობით, შეიძლება გაუტეხონ ელფოსტის ანგარიშები. ამიტომ, როცა მიიღებთ მოულოდნელ მეილს დანართით, კარგი იქნება, თუ გახსნამდე წერილის სავარაუდო ავტორთან მის ნამდვილობას გადაამოწმებთ.

- **შეამოწმეთ ბმულები დაწკაპუნებამდე**

არ დააწკაპუნოთ ბმულებზე, რომლებიც მიიღეთ იმ პირებისგან ან ორგანიზაციებისგან, ვისგანაც წერილს არ ელოდებით. თითოეული მიღებული ბმული გადაამოწმეთ და შეხედეთ მათ, როგორც პოტენციურ რისკებს. როდესაც მიიღებთ გაფრთხილებას კოლეგისგან, თქვენი ბანკისგან ან სოციალური მედიის სერვისისგან, რომელსაც იყენებთ, არ დააწკაპუნოთ ბმულზე ელფოსტაში. გადაატარეთ მაუსი ბმულზე, რათა ნახოთ ვებსაიტის სრული მისამართი. ეს დაგეხმარებათ გაარკვიოთ, გსურთ, თუ არა დააწკაპუნოთ ამ ბმულზე. გარდა ამისა, შეგიძლიათ გახსნათ ბრაუზერის ფანჯარა და მისამართი აკრიფოთ პირდაპირ URL ველში, რათა დარწმუნდეთ, რომ საიტი ნამდვილია.

დაასკანერე UnshortenIt

სანამ დააწკაპუნებთ ბმულზე, რომელიც ოდნავ მაინც საეჭვოდ მიგაჩნიათ, დაასკანერეთ იგი ბმულების სკანერით. მაგალითად, Norton Safe Web-ით, რომელიც საშუალებას გაძლევთ შეიყვანოთ საეჭვო ბმულის URL და შეამოწმოთ მისი უსაფრთხოება.

განსაკუთრებული სიფრთხილე გამოიჩინეთ, როდესაც საქმე გაქვთ შემოკლებულ URL ბმულებთან. ყოველთვის შეამოწმეთ შემოკლებულის მიღმა არსებული რეალური URL ბმული. შემოკლებული URL-ის „გასაშიფრად“ შეგიძლიათ, გამოიყენოთ უფასო ონლაინ-სერვისი, მაგალითად, UnshortenIt.

დაასკანერე Norton Safe Web

- **ნუ იჩქარებთ, დაფიქრდით**

ფიშინგის ერთ-ერთი ტაქტიკა, რომელსაც კრიმინალები და თაღლითები განსაკუთრებით კარგად იყენებენ, გულისხმობს ცრუ გადაუდებლობის შეგრძნების შექმნას. ისინი ხანმოკლე „დედლაინს“ გიწესებენ, გაჩქარებენ და ხანდახან სასჯელითაც გემუქრებიან, თუკი მათ „შეთავაზებას“ დროულად არ უპასუხებთ. მათ შეიძლება მოგთხოვონ ჯარიმის გადახადა თქვენს ბოლო საგადასახადო დეკლარაციაში „შეცდომის“ დაშვებისთვის და მიუთითონ, რომ წინააღმდეგ შემთხვევაში სისხლისსამართლებრივი დევნა დაგემუქრებათ. ან ვინმემ, ვინც თავს თქვენს უფროსად მოგაჩვენებთ, შეიძლება მოგთხოვოთ ფულის გადარიცხვა კონკრეტულ საბანკო ანგარიშზე და დაგემუქროთ სამსახურიდან განთავისუფლებით.

ყოველთვის შეხედეთ ინფორმაციის ან ფინანსური გადარიცხვების „გადაუდებელ“ მოთხოვნებს, როგორც ძალიან საეჭვოს. დაფიქრდით, არის შანსი, რომ საგადასახადო ორგანომ დაგირეკოთ თქვენს მობილურ ტელეფონზე და მოგთხოვოთ ჯარიმის გადახდა? მოგთხოვდათ თუ არა თქვენი უფროსი ოდესმე ფულის ჩარიცხვას საბანკო ანგარიშზე? თუ რამე საეჭვოდ გეჩვენებათ, დაელაპარაკეთ მას, ვისაც ენდობით, მაგალითად, კოლეგას ან ადვოკატს.

- **გადაამოწმეთ პირების ვინაობა**

ყოველთვის დარწმუნდით, რომ ადამიანები ან ორგანიზაციები, რომლებიც ითხოვენ ინფორმაციას ან ფინანსურ გადარიცხვებს, ნამდვილები არიან. დაურეკეთ მათ პირდაპირ ან დაუკავშირდით მესენჯერით. გახსოვდეთ, რომ თაღლითები ძალიან ოსტატურად იპარავენ სხვების ვინაობას, წინასწარ კვლევას ატარებენ და თქვენ მოსატყუებლად დიდ ძალისხმევას ხარჯავენ.

- **დროულად განაახლეთ თქვენი ანტივირუსი**

მაშინაც კი, თუ უკიდურესად ფრთხილი ხართ და სრულყოფილად იცავთ ციფრულ „ჰიგიენას“, ყოველთვის გააქტიურეთ ანტივირუსი და firewall ყველა მოწყობილობაზე, რომელსაც იყენებთ. ხშირად განაახლეთ თქვენი ანტივირუსი, რათა ის გაუმკლავდეს ნებისმიერ ახალ

საფრთხეს. კარგი იქნება, თუ თქვენს კრიტიკულად მნიშვნელოვან პროგრამულ უზრუნველყოფას, მაგალითად ანტივირუსს და ოპერაციულ სისტემას, ავტომატურ განახლებაზე დააყენებთ.

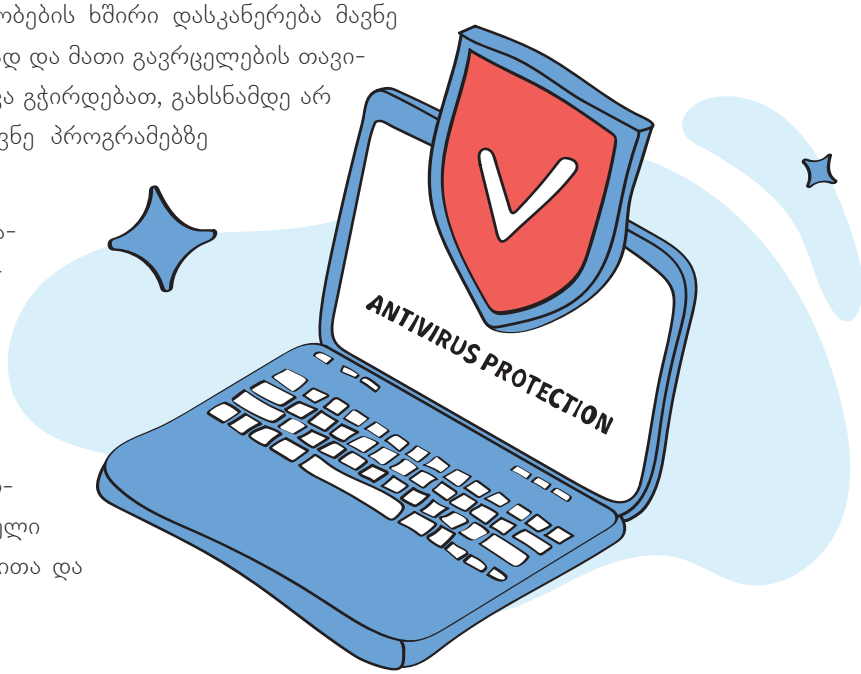
როგორ დავიცვათ თავი მავნე პროგრამებისგან

ერთ-ერთი ყველაზე გავრცელებული გზა, რომლითაც ჰაკერები და კრიმინალები ქმნიან პრობლემებს ინტერნეტში, არის მავნე პროგრამების გავრცელება. მიჰყევით ამ ძირითად მითითებებს, რათა დაიცვათ თავი მავნე პროგრამებისგან.

- **გამოიყენეთ ანტივირუსი**

თქვენს მოწყობილობაზე ყოველთვის გქონდეთ ჩართული სანდო ანტივირუსული პროგრამა. ეს პროგრამა არის თქვენი მთავარი თავდაცვის ხაზი ვირუსებისა და სხვა სახის მავნე პროგრამებისგან. რეგულარულად განაახლეთ თქვენი ანტივირუსი, რათა გაუმკლავდეს ნებისმიერ ახალ საფრთხეს.

ანტივირუსული პროგრამები საშუალებას გაძლევთ, სრულად დაასკანეროთ თქვენი მოწყობილობა მავნე პროგრამებზე. გაითავისეთ მოწყობილობების ხშირი დასკანერება მავნე პროგრამების ადრეულ ეტაპზე გამოსავლენად და მათი გავრცელების თავიდან ასაცილებლად. თუ რაიმეს ჩამოტვირთვა გჭირდებათ, გახსნამდე არ დაგავიწყდეთ ჩამოტვირთული ფაილის მავნე პროგრამებზე დასკანერება.



Windows-ს გააჩნია ჩაშენებული უფასო და საიმედო ანტივირუსული პროგრამული უზრუნველყოფა – Microsoft Defender.

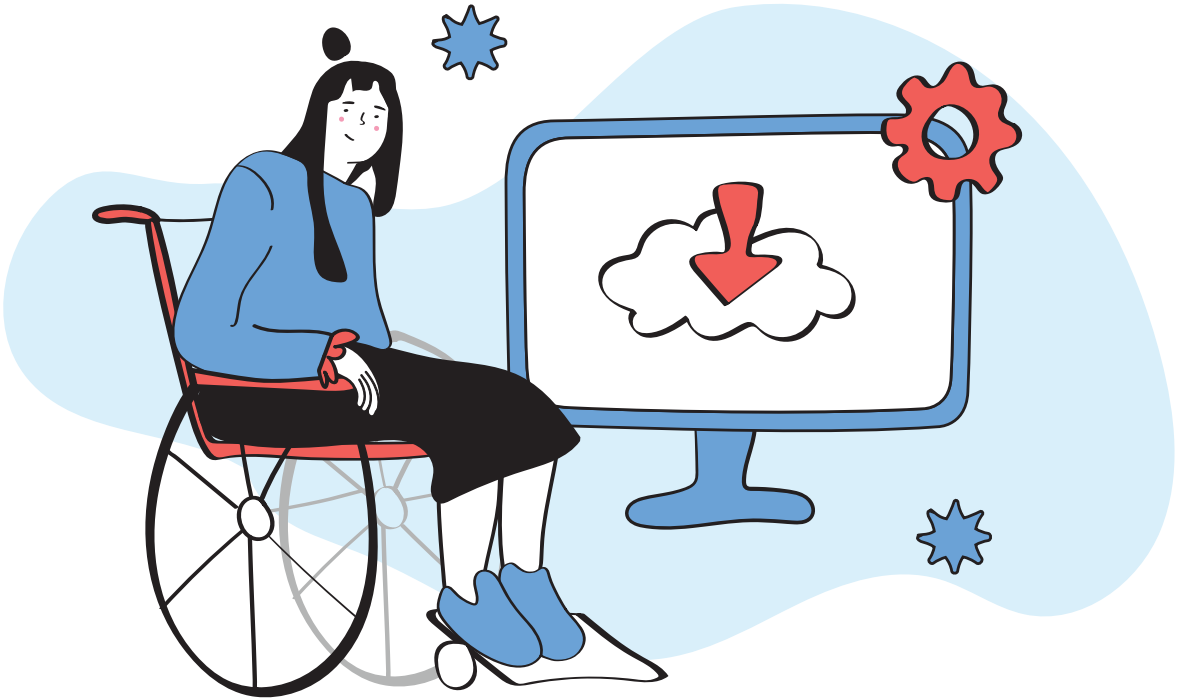
- **რეგულარულად განაახლეთ თქვენი პროგრამული და ტექნიკური უზრუნველყოფა**

მავნე პროგრამული უზრუნველყოფა აინფიცირებს თქვენს მოწყობილობებს, პროგრამული უზრუნველყოფის დაუცველობების აღმოჩენითა და

მათი გამოყენებით. ჰაკერები და კრიმინალები მუდმივად ეძებენ ასეთ დაუცველობებს. კომპანიები, რომლებიც ქმნიან პროგრამულ უზრუნველყოფას, ასწორებენ დაუცველობებს განახლებებად გამოქვეყნებული უსაფრთხოების პატჩების მეშვეობით. ამიტომ, მნიშვნელოვანია დააყენოთ განახლებები, როგორც კი ისინი გამოვა.

რომელ მოწყობილობასაც არ უნდა იყენებდეთ, დარწმუნდით, რომ იყენებთ ოპერაციული სისტემის უახლეს ვერსიას. კარგი იქნება, თუ დააყენებთ ოპერაციულ სისტემასა და ანტივირუსულ პროგრამას ავტომატურ განახლებაზე. ხშირად და რეგულარულად განაახლეთ ყველა სხვა პროგრამული უზრუნველყოფა თქვენს მოწყობილობებზე.

თუ ბოლო ექვსი თვის განმავლობაში თქვენს მობილურ ტელეფონზე ოპერაციული სისტემის განახლებები არ ყოფილა, დიდი ალბათობით, ეს ძველი მოდელია, რომელსაც მწარმოებელი აღარ უწევს მხარდაჭერას. ამ შემთხვევაში, იფიქრეთ ტელეფონის შეცვლაზე უფრო ახალი მოდელით, რომელიც იღებს უსაფრთხოების მნიშვნელოვან განახლებებს.

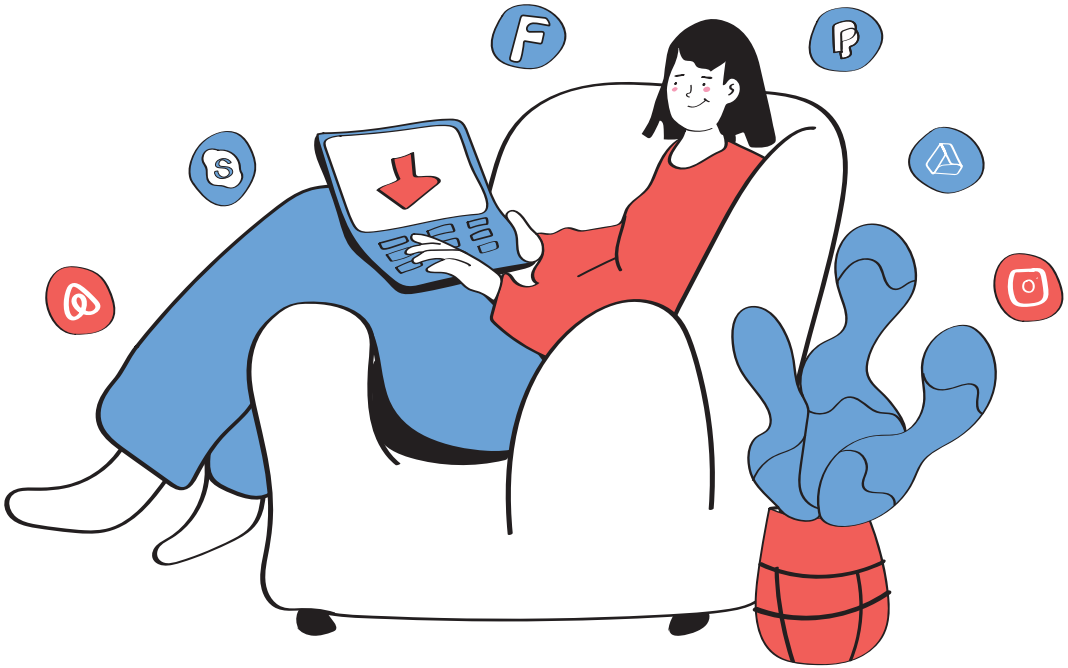


- **გამოიყენეთ ანგარიში, რომელსაც არ გააჩნია ადმინისტრატორის უფლებები**

მავნე პროგრამული უზრუნველყოფა შეიძლება დამღუპველი აღმოჩნდეს თქვენი მოწყობილობისთვის და მასზე არსებული მონაცემებისთვის, თუ ადმინისტრატორის ანგარიშით შედიხართ სისტემაში. კარგი იქნება, თუ თქვენს კომპიუტერზე შექმნით მომხმარებლის ანგარიშს შეზღუდული პრივილეგიებით და გამოიყენებთ მას რეგულარული და ყოველდღიური ამოცანებისთვის. როდესაც შედიხართ შეზღუდული პრივილეგიების მქონე ანგარიშით, მავნე პროგრამებისთვის გაცილებით უფრო რთულია იპოვონ გზა თქვენს მოწყობილობაში შესაღწევად და განახორციელონ ცვლილებები მთელი სისტემის მასშტაბით.

- **იცოდეთ, რა პროგრამებს აინსტალირებთ**

ბევრი მავნე პროგრამა შეფუთულია ჩრდილოვან პროგრამულ უზრუნველყოფასთან ერთად ან ჩაშენებულია ლეგალური პროგრამული უზრუნველყოფის პირატულ ვერსიებში. თქვენი კომპიუტერის მავნე პროგრამით დაინფიცირების ერთ-ერთი ყველაზე „საიმედო“ გზა მასზე პირატული (არალიცენზირებული) პროგრამული უზრუნველყოფის დაყენებაა. თუ ნამდვილად გჭირდებათ პროგრამული უზრუნველყოფის



კონკრეტული ნაწილი, მაგრამ არ გაქვთ ამის საშუალება, გაითვალისწინეთ, რომ არსებობს თითქმის ყველა ძირითადი პროგრამული პროდუქტის უფასო ალტერნატივა. შესაძლოა ეს ალტერნატივები სთავაზობენ უფრო შეზღუდულ ფუნქციონირებას, მაგრამ ისინი ასრულებენ სამუშაოს ისე, რომ მავნე პროგრამასთან ერთად მუდმივი „ონლაინ თანაცხოვრება“ არ მოგიხდეთ. როდესაც შესაძლებლობა გაქვთ, ყოველთვის აირჩიეთ ღია კოდის მქონე პროგრამული უზრუნველყოფა, პატენტური კომერციული პროდუქტების ნაცვლად.

ჩამოტვირთეთ აპლიკაციები მხოლოდ აპლიკაციების ოფიციალური მაღაზიებიდან. როდესაც რაიმეს პირველად აინსტალირებთ და არ იცნობთ აპლიკაციას, აუცილებლად წაიკითხეთ განხილვები კომენტარებში, რათა გაარკვიოთ, თვლიან თუ არა სხვა მომხმარებლები იმ პროგრამულ უზრუნველყოფას სანდოდ.

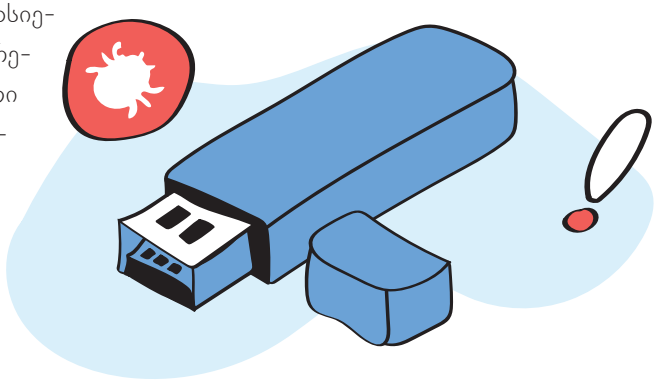
ჩვეულებად აქციეთ თქვენს მოწყობილობებზე დაინსტალირებული ყველა აპლიკაციის რეგულარული განახლება. წაშალეთ აპლიკაციები, რომლებსაც აღარ იყენებთ ან არ ენდობით.

- **არ ენდოთ ამოსახტომ შეტყობინებებს**

ყველას გვქონია ასეთი შემთხვევა: ათვალიერებთ რაღაცას ინტერნეტში და უცებ გაჩენილა ფანჯარა, რომელშიც გეუბნებიან, რომ თქვენი კომპიუტერი დაინფიცირებულია და გირჩევთ ჩამოტვირთოთ გარკვეული პროგრამა თქვენი მოწყობილობის დასაცავად. ნუ წამოეგებით ამ მახეს. ფრთხილად იყავით. როგორც წესი, მსგავსი პროგრამა თვითონ არის ვირუსი, რომელიც შესაძლოა ძალიან დიდი საფრთხის შემცველი იყოს თქვენი მოწყობილობისთვის.

- **ფრთხილად იყავით მოსახსნელ მედია-მატარებლებთან**

მავნე პროგრამები ხშირად მოგზაურობენ სხვადასხვა მოწყობილობებში მოსახსნელი მედია-მატარებლების საშუალებით, ისეთების, როგორიცაა USB მეხსიერების დისკები, გარე მყარი დისკები, ფლეშ-მეხსიერების ბარათები და ა. შ. არასოდეს შეუერთოთ ასეთი მოწყობილობა თქვენს კომპიუტერს, თუ არ იცით საიდან გაჩნდა თქვენთან. როდესაც თქვენ გჭირდებათ მოსახსნელი მედია-მოწყობილობის გამოყენება და იცით საიდან მოხვდა თქვენთან, კარგი იქნება, თუ მის გახსნამდე, მაინც გამოიყენებთ ანტივირუსულ პროგრამას მისი სკანირებისთვის.

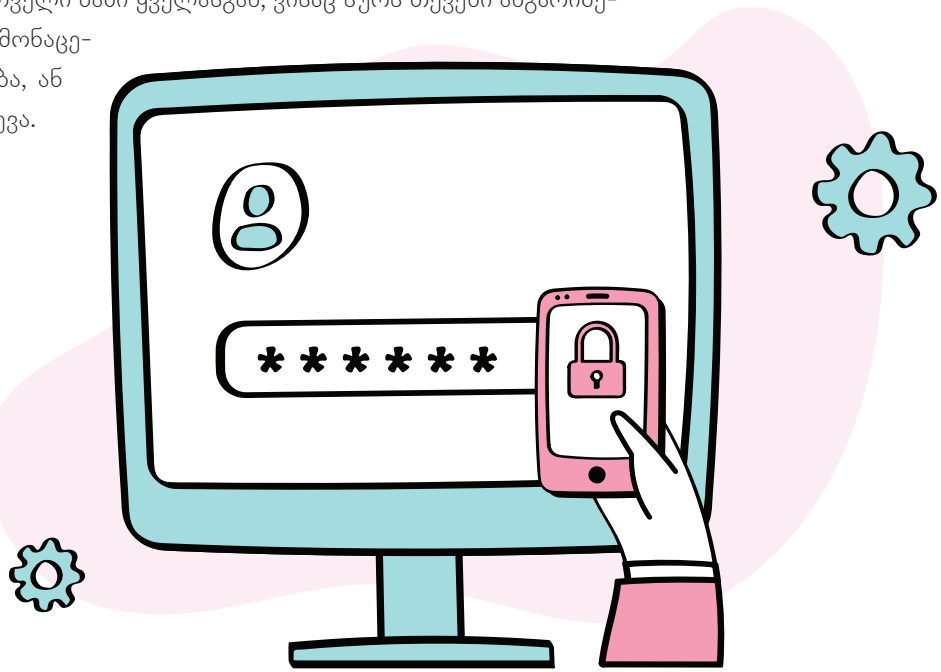


თავი 2. პაროლები

ინდივიდები და ორგანიზაციები იყენებენ პაროლებს მნიშვნელოვანი ანგარიშების, მოწყობილობების, ქსელების და მონაცემების დასაცავად. ამ დროს, ბოროტმოქმედები მუდმივად პოულობენ ახალ გზებს პაროლების გამოსაცნობად ან მათ მოსაპარად. ძლიერი პაროლების შექმნა, მათი უსაფრთხოდ მართვა და ორნაბიჯიანი ავტორიზაციით (2FA) მათი გაძლიერება, უმნიშვნელოვანესი ნაბიჯებია ციფრული უსაფრთხოების დასაცავად.

ჩვენი პირადი და პროფესიული ცხოვრება სულ უფრო მეტად უკავშირდება ონლაინ ანგარიშებს. ელფოსტა, სოციალური მედია, ფაილების გაზიარება, შეტყობინებების გაგზავნა, ვიდეოს ყურება, ბანკინგი, შოპინგი, მონაცემების სარეზერვო ასლების შექმნა – ყველა ამ სერვისისთვის ანგარიშის ქონაა საჭირო. შედეგად, გიწევთ ათობით სხვადასხვა ანგარიშის დამახსოვრება და დაცვა.

პაროლები არის თქვენი დაცვის პირველი ხაზი ყველასგან, ვისაც სურს თქვენი ანგარიშების მოპარვა, თვალთვალი, თქვენი მონაცემების თუ დოკუმენტების გამოყენება, ან უბრალოდ თქვენს ანგარიშში შეღწევა.



როგორ შევქმნათ ძლიერი პაროლები

ანგარიშების დასაცავად ყველა პაროლი თანაბრად კარგი არ არის. ასობით მილიონი მომხმარებელი მთელ მსოფლიოში კვლავ იყენებს პაროლებს, რომელთა გამოცნობა ან გატეხვა ძალიან ადვილია. გავიდა ის დრო, როდესაც პაროლებს გატეხვა მხოლოდ ყველაზე ჭკვიან ჰაკერებს შეეძლოთ. ამისთვის კი მრავალწლიანი გამოცდილება, უნიკალური უნარები და ხელსაწყოები იყო საჭირო. დღეს პაროლების უმეტესობა ტყდება ყველასთვის ხელმისაწვდომი პროგრამული უზრუნველყოფის საშუალებით. იგი არჩევს ცნობილი სიტყვებისა და სიმბოლოების სხვადასხვა კომბინაციებს მანამ, სანამ არ იპოვის სწორ შესატყვისს. პაროლის გატეხვის ეს მეთოდი ითარგმნება როგორც უხეში ძალის შეტევა (Brute force attack).

ასე რომ, როგორც ინდივიდებს და როგორც საჯარო მოხელეებს, განსაკუთრებით მათ, ვისაც წვდომა გაქვთ საჯარო სამსახურში არსებულ ინფორმაციასთან, ანგარიშებისა და მათში არსებული ინფორმაციის დასაცავად გჭირდებათ ძლიერი პაროლები. ანუ მათი გატეხვა ძალიან რთული უნდა იყოს. მარტივად რომ ვთქვათ, უხეში ძალის ინსტრუმენტებს მათ გასატეხად ძალიან დიდი დრო უნდა სჭირდებოდეთ. იმდენად დიდი, რომ ბოროტმოქმედი საბოლოოდ უარს ამბობდეს ანგარიშის გატეხვაზე.

შექმენით რთულად გასატეხი პაროლი

- **თქვენი პაროლი უნდა იყოს გრძელი**

ეს ყველაზე მნიშვნელოვანი ფაქტორია. გამოიყენეთ მინიმუმ 12 სიმბოლო ან უფრო მეტი, თუ ეს შესაძლებელია.

- **სიმბოლოები გამოიყენეთ შერეულად**

რაც უფრო მეტ „დიდ“ და „პატარა“ ასოს, რიცხვსა და სიმბოლოს გამოიყენებთ, მით უფრო რთული იქნება თქვენი პაროლის გატეხვა. შემთხვევითი სიმბოლოებისგან შემდგარი პაროლები ბევრად უფრო ძლიერია, ვიდრე სიტყვების შემცველი პაროლები. ასე რომ, პაროლი *iLoVeYOu56&#* უფრო ძლიერია, ვიდრე *iloveyou9!*, მაგრამ, ბევრად უფრო უსაფრთხო ვარიანტი იქნება *iL3*Ov50&0Ey6824(2uO*.

- **არ გამოიყენოთ კლავიატურის დასამახსოვრებელი კომბინაციები ან აშკარა სიტყვები**

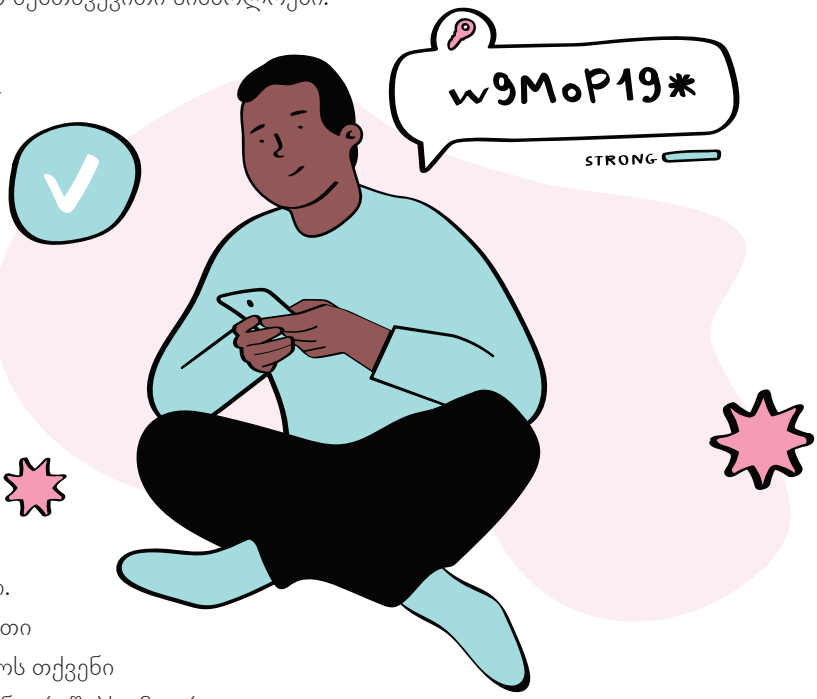
ისეთი პაროლები, როგორიცაა *qwerty*, *12345678*, *password123* და *myemailpass* ყველაზე მარტივი გასატეხია.

- **მოერიდეთ სიმბოლოების აშკარა ჩანაცვლებებს**

მიუხედავად იმისა, რომ სიმბოლოების ჩანაცვლება პაროლებს აძლიერებს, ერიდეთ სიმბოლოების ყველაზე აშკარა ჩანაცვლებებს. *D00RB3LL* მცირედით უკეთესია ვიდრე *DOORBELL*, მაგრამ მისი გატეხვა მაინც ძალიან ადვილია. ამის ნაცვლად გამოიყენეთ შემთხვევითი სიმბოლოები.

- **არ გამოიყენოთ პირადი ინფორმაცია**

თუ საფრთხეში ხართ და ვიღაცას თქვენი ანგარიშის გატეხვა უნდა, მაშინ ჰაკერი პაროლის გამოცნობისას აუცილებლად გამოიყენებს ნებისმიერ ინფორმაციას, რომელიც თქვენ შესახებ გააჩნია. ის არ უნდა მოიცავდეს თქვენი ძაღლის სახელს, ქალაქს, სადაც დაიბადეთ, სპორტულ გუნდს, რომელსაც გულშემატკივრობთ, თქვენი შვილის სახელს, დაბადების თარიღს და ა. შ.



- **არ გამოიყენოთ ერთი და იგივე პაროლები**

ყველა თქვენს ანგარიშსა და მოწყობილობას უნდა ჰქონდეს საკუთარი უნიკალური პაროლი. თუ ვინმე მოგპარავთ ან გაგიტეხავთ ერთ-ერთი ანგარიშის პაროლს, ის აგრეთვე შეეცდება გატეხოს თქვენი ყველა სხვა ანგარიშიც. ბოროტმოქმედი ეცდება ანგარიშებს „მოარგოს“ მოპარული პაროლი და მისი სხვადასხვა ვარიაცია.

შეიძლება იფიქროთ, რომ თქვენი თითოეული ანგარიშისთვის უნიკალური პაროლის ქონა და მათ სიძლიერეზე ზრუნვა ზედმეტია. რა დაიმახსოვრებს ყველა ამ პაროლს? თქვენ მხოლოდ ერთი ძლიერი პაროლის დამახსოვრება მოგეთხოვებათ. დანარჩენს თქვენ მაგივრად პაროლების მენეჯერი გააკეთებს.

რატომ და როგორ უნდა გამოვიყენოთ პაროლების მენეჯერები

თქვენი ანგარიშების დასაცავად, უნდა გამოიყენოთ ძლიერი პაროლები, რომლებიც ჩვეულებრივ შეიცავს სიმბოლოების გრძელ და შემთხვევით კომბინაციებს. ასეთი პაროლების დამახსოვრება თითქმის შეუძლებელია. გარდა ამისა, უნდა გქონდეთ უნიკალური პაროლი თითოეული ანგარიშისთვის.

როგორ უნდა დაიმახსოვროთ და შეინახოთ ყველა ეს პაროლი? გამოსავალი პაროლების მენეჯერია.

იფიქრეთ პაროლების მენეჯერზე, როგორც სეიფზე, სადაც შეინახავთ ათობით ან თუნდაც ასობით გასაღებს (პაროლს) ყველა თქვენი ანგარიშისთვის. ეს გაგიმარტივებთ ცხოვრებას, რადგან დაგჭირდებათ მხოლოდ ერთი პაროლის დამახსოვრება პაროლების მენეჯერში შესასვლელად. იქ ყველა თქვენს პაროლს შეინახავთ.

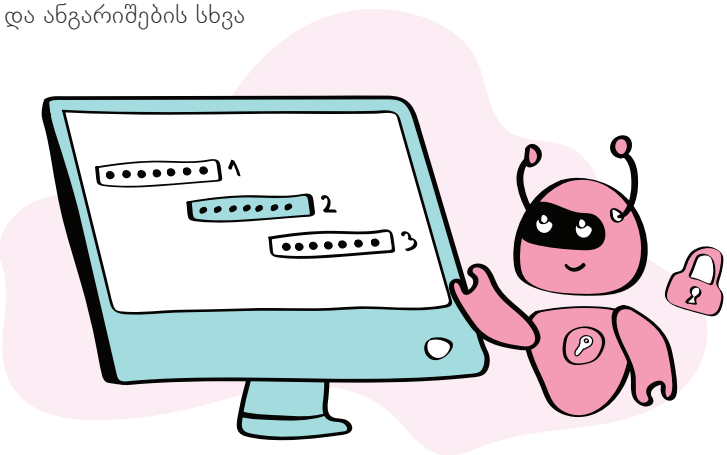
რას აკეთებს პაროლების მენეჯერი?

- **ინახავს თქვენი ანგარიშების მონაცემებს**

სავარაუდოდ, გაქვთ ათობით ან თუნდაც ასობით სხვადასხვა ონლაინ ანგარიში. ყველა ამ ანგარიშის (მომხმარებლის სახელების, ელფოსტის მისამართებისა და პაროლების) მონაცემების ფურცელზე ჩამოწერა, ან კომპიუტერში შენახვა ძალიან ცუდი აზრია. პაროლების მენეჯერი აიოლებს ყველა ამ ანგარიშის შენახვას. ის იმახსოვრებს თქვენს ყველა პაროლს და ანგარიშების სხვა მონაცემებს.

- **ინახავს მათ უსაფრთხოდ**

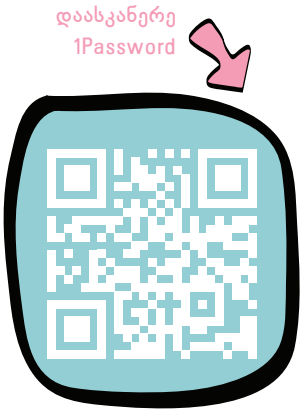
პაროლების მენეჯერში ყველა თქვენი პაროლის შენახვა ბევრად უფრო უსაფრთხოა. არავის შეუძლია გახსნას თქვენი პაროლების მენეჯერი, თუ მას ძალიან ძლიერი პაროლით იცავთ. დამატებითი სიფრთხილისთვის, გამოიყენეთ ორნაბიჯიანი ვერიფიკაცია თქვენი პაროლების მენეჯერის დასაცავად.

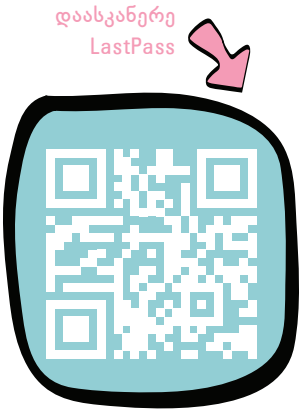


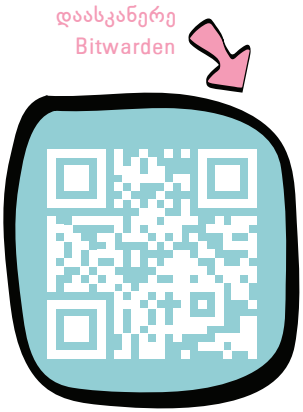
- ქმნის ძლიერ, უნიკალურ პაროლებს

პაროლების მენეჯერი, ასევე, აიოლებს ძლიერი პაროლების შექმნას. მისი წყალობით ყველა ანგარიშზე უნიკალური პაროლი გექნებათ. პაროლების მენეჯერი პაროლებს ქმნის თქვენ ნაცვლად. ამასთან, საშუალებას გაძლევთ, აკონტროლოთ თქვენი პაროლების სიგრძე და სირთულე.

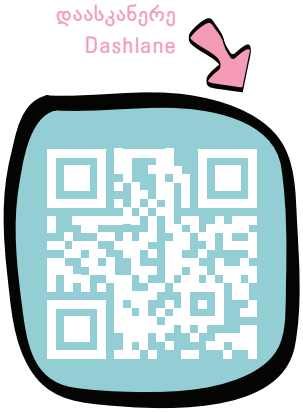
რომელი პაროლების მენეჯერი უნდა გამოიყენოთ?

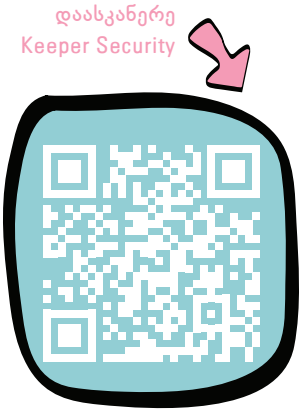


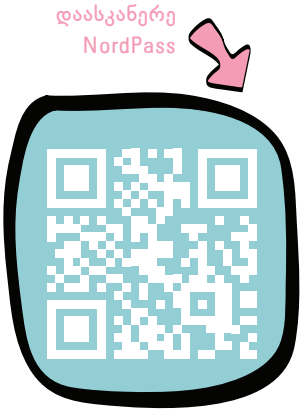




პაროლების მენეჯერი შეგიძლიათ მოარგოთ თქვენს საჭიროებებსა და მოთხოვნებს. არსებობს რამდენიმე საიმედო და უსაფრთხო ვარიანტი. თუ გადაწყვეტთ გადაიხადოთ გამოწერის საფასური, მაშინ უსაფრთხო ვარიანტებია: 1Password, LastPass, Bitwarden, Dashlane, Keeper Security, NordPass.







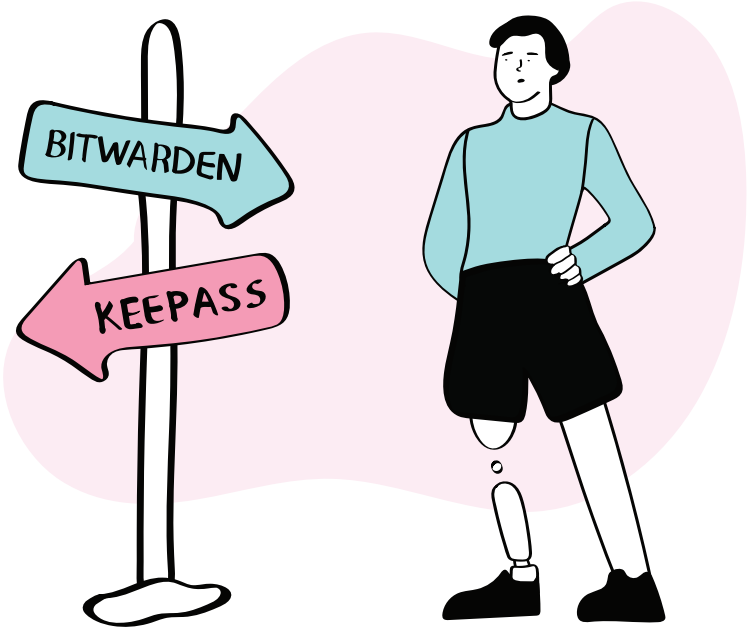
დაასკანერე
KeePass

პაროლების ზოგიერთი მენეჯერი, ასევე, სთავაზობს უფასო სერვისს მომხმარებლებს, რომლებსაც არ სჭირდებათ მოწინავე ფუნქციები. თუ გადაწყვეტთ უფასო პაროლების მენეჯერის გამოყენებას, ყველაზე უსაფრთხო ღია კოდის მქონე პროგრამის არჩევაა. მაგალითად: BitWarden, KeePass, KeePassXC.

დაასკანერე
KeePassXC

პაროლების მენეჯერები იყოფიან ორ ზოგად კატეგორიად, იმის მიხედვით, თუ სად ინახავენ მომხმარებლების ანგარიშების მონაცემებს. თუ იყენებთ ლოკალურ პაროლების მენეჯერს, როგორიცაა KeePassXC, ის ინახავს პაროლებს თქვენს მოწყობილობაზე. ასეთი პაროლების მენეჯერები გვთავაზობენ უკეთეს კონფიდენციალურობას და უსაფრთხოებას, მაგრამ მათ სჭირდებათ გარკვეული დონის ტექნიკური ცოდნა და ციფრული „ჰიგიენა“ მათი უსაფრთხოდ გამოსაყენებლად.

საპირწონედ, *ღრუბლოვანი* პაროლების მენეჯერები ინახავენ პაროლებს ღრუბლოვან სერვერებზე. ეს ვარიანტი უფრო უსაფრთხოა იმ მომხმარებლებისთვის, რომლებსაც აქვთ შეზღუდული ტექნიკური ცოდნა და არ შეუძლიათ მკაცრი ციფრული „ჰიგიენის“ დაცვა, რომელიც



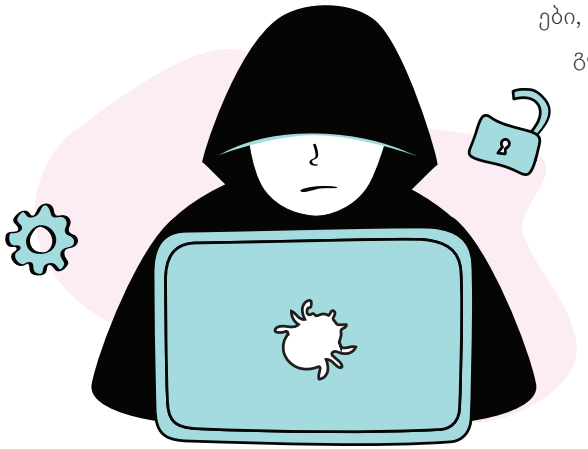
მოიცავს ავტომატური სარეზერვო ასლების გაკეთებას. ორივე – BitWarden და KeePass – უფასო ღრუბელოვანი პაროლების მენეჯერია, ღია საწყისი კოდით, რომლებიც ცნობილები არიან მათი უსაფრთხოებისა და საიმედოობის გამო.

რატომ უნდა იყოს ყველა თქვენი პაროლი უნიკალური

ყველა თქვენს ანგარიშს უნდა ჰქონდეს უნიკალური პაროლი, რომელიც აქამდე არასდროს გამოგიყენებიათ. მსოფლიოში ყველაზე ძლიერი პაროლი რომც გქონდეთ, მას თუ სხვადასხვა ანგარიშისთვის გამოიყენებთ, ამით საკუთარ თავს და სამსახურეობრივ ანგარიშებს დიდ საფრთხეში ააგდებთ.

რა ხდება, როდესაც ხელახლა იყენებთ იგივე პაროლს?

ვთქვათ, რომ იგივე პაროლს იყენებთ თქვენი ელფოსტის, Facebook-ისა და Instagram- ისთვის. თუ თქვენი ელფოსტის პროვაიდერი ვერ შეძლებს უსაფრთხოების უზრუნველყოფას (ეს კი იმაზე ხშირად ხდება, ვიდრე ვაცნობიერებთ) და თქვენი ანგარიშის მონაცემებს მოიპარავენ, თაღლითები ეცდებიან გამოიყენონ მოპარული პაროლი და მისი ოდნავ შეცვლილი ვერსიები, რათა შეაღწიონ იმ ანგარიშებშიც, რომელიც სხვა საიტებზე გაქვთ. ანუ, გაგიტეხავენ ყველა ანგარიშს, სადაც ერთსა და იმავე პაროლს იყენებთ.



პაროლების ხელახლა გამოყენება ასევე ცუდი აზრია, რადგან, მილიონობით სხვა მომხმარებლის მსგავსად, თქვენც გექნებათ ანგარიშები, რომლებიც ადრე შექმენით და ახლა მათი არსებობა აღარც გახსოვთ. დიდი შანსია, რომ ამ ანგარიშებიდან ზოგი მაინც იყოს გატეხილი. თუ თაღლითს აქვს ამ ანგარიშებთან დაკავშირებული ელ ფოსტის მისამართი, მისი მეშვეობით ყველა გატეხილ ანგარიშს მარტივად

დაასკანერე
pwned

იპოვის. ასევე, ადვილია ყველა ასეთი ანგარიშის „გაჟონილი“ პაროლების მოპოვება. ასე რომ, თუ თქვენ იყენებთ იგივე პაროლს ან მის ოდნავ შეცვლილ ვერსიებს რამდენიმე ანგარიშისთვის, თაღლითს შეუძლია გატეხოს ისინი თქვენი ერთი დავიწყებული ანგარიშის პოვნით. ამას ეწოდება პაროლის ჩატენვა.

- თუ გსურთ, შეამოწმოთ, არის თუ არა თქვენი ელფოსტის მისამართ(ებ)ი დაკავშირებული რომელიმე „გაჟონილ“ ანგარიშთან, შეგიძლიათ გამოიყენოთ ეს სერვისი. უბრალოდ ჩაწერეთ ელფოსტის მისამართი საძიებო ველში და დააწკაპუნეთ “pwned?”-ზე.
- თუ ელფოსტის მისამართმა „გაჟონა“, თქვენ მიიღებთ ყველა ონლაინ სერვისის ჩამონათვალს, სადაც თქვენი ანგარიშის მონაცემები რაიმე სახით იყო კომპრომეტირებული. შედით თითოეულ ამ ანგარიშში და შეცვალეთ თქვენი პაროლები, რაც შეიძლება მალე. ასევე, განიხილეთ თქვენი მნიშვნელოვანი ანგარიშების დაცვა ორნაბიჯიანი ვერიფიკაციით. გახსოვდეთ, თქვენი პაროლები უნდა იყოს ძლიერი და უნიკალური. თუ ამ ანგარიშებიდან არცერთს აღარ იყენებთ, მაშინ დაფიქრდით მათ წაშლაზე.

რატომ უნდა გამოიყენოთ ორნაბიჯიანი ავტორიზაცია

სამწუხაროდ, ყველაზე ძლიერი პაროლიც კი, ბოლომდე ვერ დაგიცავთ ანგარიშის გატეხვისგან. თქვენი პაროლის გასატეხად რამდენიმე გზა არსებობს. ჰაკერებმა შეიძლება მოიპარონ თქვენი პირადი მონაცემები უშუალოდ ონლაინ სერვისის პროვაიდერისგან (რაც იმაზე ხშირად ხდება, ვიდრე გგონიათ). ვიღაცამ შეიძლება დააინსტალიროს თქვენს მოწყობილობაზე პაწაწინა პროგრამული უზრუნველყოფა, რომელიც ჩაიწერს თქვენს კლავიატურაზე ყველა ღილაკის დაჭერას (მათ შორის, ყველა თქვენს პაროლს). ძალიან სანდო ადამიანმა შეიძლება გატეხოს თქვენი პაროლი ან დაგარწმუნოთ მის გამჟღავნებაში, ან სულაც, შეიძლება ფიშინგის მსხვერპლი გახდეთ და საკუთარი ხელით შეიყვანოთ თქვენი პაროლი არასაჭირო ადგილას.

სწორედ ამიტომ, გამოიყენეთ ორნაბიჯიანი ავტორიზაცია (2FA) თქვენი ციფრული ანგარიშების დასაცავად. როდესაც ჩართულია ორნაბიჯიანი ავტორიზაცია, ონლაინ ანგარიშზე წვდომისთვის თქვენი ვინაობა ორი განსხვავებული გზით უნდა დაადასტუროთ. ამრიგად, პაროლის შეყვანის გარდა (*პირველი* ფაქტორი), თქვენ უნდა გააგზავნოთ მეორე სახის ინფორმაცია (*მეორე* ფაქტორი) თქვენი ვინაობის დასადასტურებლად. სინამდვილეში, 2FA უზრუნველყოფს თქვენი ონლაინ ანგარიშების დაცვის კიდევ ერთ ფენას. ისინი დაცულია, მაშინაც კი, როდესაც თქვენი პაროლები გატეხილია.

რა შეიძლება გახდეს მეორე ფაქტორი?

ონლაინ ანგარიშების უმეტესობა მომხმარებლებს საშუალებას აძლევს აირჩიონ ვერიფიკაციის სამი დამატებითი ფაქტორიდან ერთ-ერთი:

- **ის, რაც მხოლოდ თქვენ იცით:** მაგ. PIN-კოდი ან პასუხი თქვენს მიერ არჩეულ უსაფრთხოების კითხვებზე.
- **ის, რაც გაქვთ:** ფიზიკური ობიექტი, რომელიც უნდა გქონდეთ ონლაინ ანგარიშებზე წვდომისთვის. ეს შეიძლება იყოს უსაფრთხოების ჟეტონი (პროგრამული უზრუნველყოფის პატარა მოწყობილობა) ან თქვენი სმარტფონი, რომელიც შეიძლება გამოიყენოთ სავერიფიკაციო კოდების მისაღებად. მოკლე ტექსტური შეტყობინებით ან სპეციალური აპლიკაციების საშუალებით.
- **თქვენი ნაწილი:** თითის ანაბეჭდი, სახე ან თვალის ბადურა.

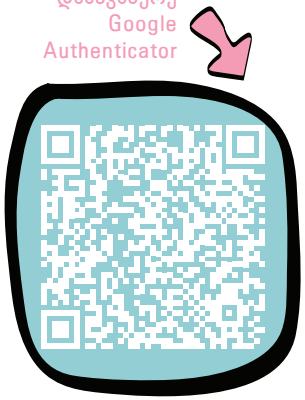
რომელი ფაქტორი უნდა აირჩიოთ?

ზოგადი რჩევის მიცემა რთულია, რადგან უნივერსალური 2FA არ არსებობს. საბოლოო ჯამში, არჩევანი უნდა გააკეთოთ სიტუაციის და რისკების შეფასებასა და იმაზე დაყრდნობით, თქვენთვის რა უფრო მოსახერხებელია. ქვემოთ მოყვანილი ინფორმაცია დაგეხმარებათ გაცნობიერებული არჩევანის გაკეთებაში:

- **უსაფრთხოების კითხვები** 2FA-ს ანუ ორნაბიჯიან ვერიფიკაციას მარტივ სამუშაოდ აქცევს, რადგან მათი ერთადერთი მოთხოვნაა დაიმახსოვროთ პასუხები წინასწარ განსაზღვრულ კითხვებზე. თუმცა, როგორც წესი, მოხერხებული თაღლითისთვის არც ისე რთულია გაიგოს ეს პასუხები (მაგ. დედის ქალიშვილობის გვარი) ან გამოგტყუოთ ისინი.
- **უსაფრთხოების ჟეტონები** (U2F-გასაღებები) არის 2FA-ს ერთ-ერთი ყველაზე უსაფრთხო მეთოდი, თუ მათ საიმედოდ შეინახავთ. ამ მოწყობილობების მთავარი მინუსი არის ის, რომ ისინი ფასიანია და

დაასკანერე Authy

დაასკანერე Google Authenticator



დაასკანერე LastPass Authenticator

შესაძლოა საჭიროებდნენ განსხვავებულ გადამყვან ადაპტერებს, სხვადასხვა მოწყობილობებზე გამოსაყენებლად. გარდა ამისა, უსაფრთხოების ჟეტონს ავტორიზაციის მეორე ფაქტორად თუ იყენებთ, ესე იგი ყოველ ჯერზე, როდესაც ონლაინ ანგარიშზე შესვლა დაგჭირდებათ, მოწყობილობა თან უნდა გქონდეთ. ამრიგად, ყოველთვის არის მისი დაკარგვის ან მოპარვის რისკი.

- **მოკლე ტექსტური შეტყობინებები** ძალიან მოსახერხებელია, რადგან ისინი მომენტალურად მოდის თქვენს მობილურ ტელეფონზე. თუმცა, ეს ერთ-ერთი ყველაზე ნაკლებად უსაფრთხო 2FA მეთოდია, რადგან მოკლე ტექსტური შეტყობინებები ადვილად შეიძლება გადამისამართდეს დაინტერესებული პირის ან თქვენი მობილური პროვაიდერის მიერ.
- **სავერიფიკაციო** ანუ საავტორიზაციო აპლიკაციების გამოყენება ყველაზე უსაფრთხო და მოსახერხებელ მეთოდად ითვლება. როდესაც ავტორიზაციის აპლიკაციას აკავშირებთ ონლაინ ანგარიშთან, ის წარმოქმნის დროებით პაროლებს, ან ციფრულ კოდებს, რომლებიც უნდა შეიყვანოთ თქვენი მთავარი პაროლის შეყვანისთანავე ონლაინ ანგარიშზე წვდომისთვის. ამ პაროლების ან კოდების „დაჭერა“ შეუძლებელია ისე მარტივად, როგორც მოკლე ტექსტური შეტყობინებების. თუმცა, ამ აპლიკაციების უსაფრთხოება მიბმულია თქვენი მობილური მოწყობილობის უსაფრთხოებაზე. მათი გამოყენება უსაფრთხო რომ იყოს, თქვენი ტელეფონიც და არჩეული აპლიკაციაც ძლიერი პაროლებით უნდა დაიცვათ. ექსპერტების მიერ რეკომენდირებული სანდო სავერიფიკაციო აპლიკაციებია: Authy, Google Authenticator, LastPass Authenticator. რომელი ვარიანტიც არ უნდა აირჩიოთ, დარწმუნდით, რომ დაცულ ადგილას ინახავთ ერთჯერად სარეზერვო კოდებს ყველა ანგარიშისთვის, რომლებსაც უკავშირებთ ვერიფიკატორის აპლიკაციას. ეს კოდები დაგჭირდებათ თქვენს ანგარიშებზე წვდომისთვის, იმ შემთხვევაში, თუ დაკარგავთ ტელეფონს აპლიკაციით.
- **ბიომეტრიული მონაცემები**, მაგალითად, თითის ანაბეჭდი, სახე ან ხმა ძალიან მოსახერხებელია, მაგრამ არა იმდენად უსაფრთხო, როგორც ხშირად ფიქრობენ. სამწუხაროდ, მრავალი პოპულარული ონლაინ სერვისი არ გვთავაზობს ბიომეტრიის გამოყენებას 2FA-სთვის.

გარდა ამისა, ბევრ მომხმარებელს არ სურს გამოიყენოს თავისი ბიომეტრიული მონაცემები, რადგან პაროლებისგან განსხვავებით, გატეხილი ბიომეტრიული მონაცემების შეცვლა შეუძლებელია. გატეხვის შემდეგ, ის რჩება გატეხილად. ონლაინ სერვისებმა შესაძლოა ასევე მიჰყიდონ თქვენი ბიომეტრიული მონაცემები მესამე მხარეებს თქვენი თანხმობის გარეშე.

თავი 3. მოწყობილობები

საჯარო მოხელეებს ციფრული მოწყობილობები – პერსონალური კომპიუტერები, ლეპტოპები, პლანშეტები და სმარტფონები – გეხმარებათ კომუნიკაციაში, ინტერნეტის გამოყენებაში, მონაცემების შექმნა-შენახვა-გაზიარებაში, ყოველდღიური სამსახურეობრივი თუ პირადი საქმიანობის წარმართვაში. მათმა დაკარგვამ, მოპარვამ, დაზიანებამ ან „გატეხვამ“ შეიძლება სერიოზული პერსონალური, პროფესიონალური, ფინანსური და რეპუტაციული ზიანი მოგიტანოთ. ციფრული უსაფრთხოების მნიშვნელოვანი ნაწილია იმის ცოდნაც, თუ როგორ უნდა დაიცვათ თქვენი ციფრული მოწყობილობები.

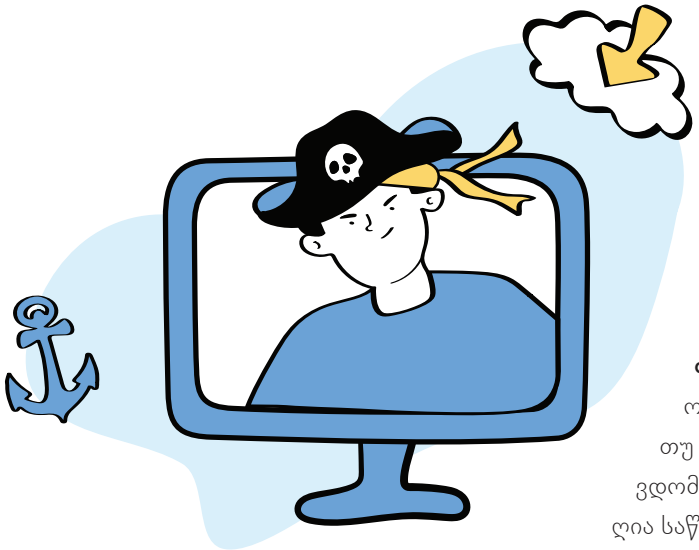
7 რჩევა საჯარო მოხელეებს კომპიუტერის უსაფრთხოების შესანარჩუნებლად

ძალიან მნიშვნელოვანია იცოდეთ, როგორ შეიძლება თქვენი კომპიუტერის დაცვა და „დაზღვევა“.

1. გამოიყენეთ მხოლოდ ლიცენზირებული პროგრამული უზრუნველყოფა

პროგრამული უზრუნველყოფა ძვირია. ამიტომაც თქვენს კომპიუტერზე არალიცენზირებული, ან „მეკობრული“ პროგრამული უზრუნველყოფის დაინსტალირება დიდი ცდუნებაა. საჯარო სამსახურისთვის იგი განსაკუთრებით რისკის შემცველია.

ასეთი პროგრამული უზრუნველყოფა იქმნება ორიგინალი აპლიკაციების ძველი ვერსიების საფუძველზე. რაც ეს ვერსიები გამოვიდა, დეველოპერებმა მათში აღმოაჩინეს და გამოასწორეს ასობით ან ათასობით შეცდომა და დაუცველობის კრიტიკულად სუსტი წერტილები. თუ იყენებთ პირატულ პროგრამულ უზრუნველყოფას, მაშინ ამ ჩასწორებებითა და განახლებებით ვერ ისარგებლებთ.



მეტიც, პირატულ პროგრამულ უზრუნველყოფას ხშირად მოჰყვება მათში უკვე ჩაშენებული მავნე კოდი. ასე რომ, არალიცენზირებული აპლიკაციების გამოყენებით, მოწყობილობაში ვირტუალურ კარს ღიას ტოვებთ. მთელი მისი შიგთავსი მუდმივად ღია იქნება კიბერკრიმინალებისთვის.

განსაკუთრებით მნიშვნელოვანია თქვენს კომპიუტერში ყველაზე მთავარი პროგრამული უზრუნველყოფის ლიცენზირებული ვერსიები გამოიყენოთ. საუბარია ოპერაციულ სისტემაზე და ანტივირუსულ პროგრამაზე. თუ კომერციული პროგრამები თქვენთვის არაა ხელმისაწვდომი, ყოველთვის შეგიძლიათ იპოვოთ უფასო ალტერნატივა ღია საწყისი კოდით.

2. ჩამოტვირთეთ პროგრამული უზრუნველყოფა მხოლოდ სანდო წყაროებიდან

კიბერკრიმინალები ხშირად ავრცელებენ პროგრამულ უზრუნველყოფას, რომელიც ჰგავს ნამდვილ აპლიკაციებს, მაგრამ მასში ჩაშენებულია სხვადასხვა ტიპის მავნე პროგრამები. ამ პროგრამული უზრუნველყოფის დაინსტალირებით კიბერდამნაშავეებს საკუთარ მოწყობილობაზე აძლევთ წვდომას.

დაასკანერე Adobe Acrobat Reader

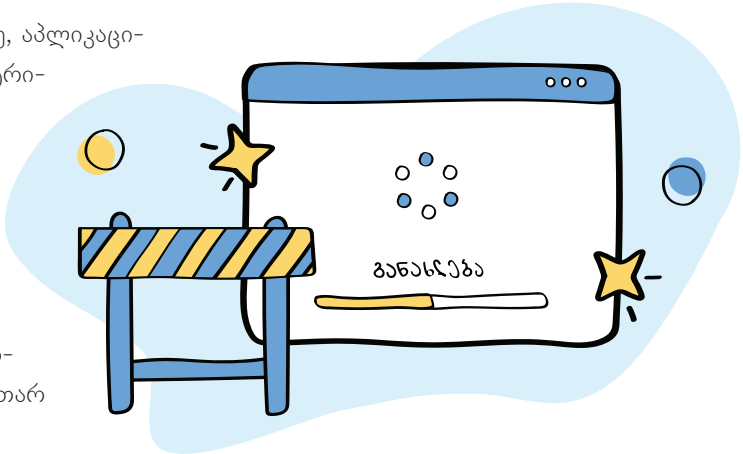
ამიტომ, **ყოველთვის ჩამოტვირთეთ პროგრამული უზრუნველყოფა და განახლებები ოფიციალური მაღაზიებიდან** (Windows მოწყობილობებისთვის Microsoft Store-დან და Mac-ისთვის App Store-დან) **ან პირდაპირ იმ კომპანიების ვებსაიტებიდან, რომლებიც ავრცელებენ აპლიკაციებსა და მათ განახლებებს**. მაგალითად, Adobe Acrobat Reader-ის დაინსტალირებისას, ჩამოტვირთეთ აპლიკაცია პირდაპირ Adobe-ის გვერდიდან და არა მესამე მხარეების ვებსაიტებიდან.

ახალი ან ნაკლებად ცნობილი პროგრამული უზრუნველყოფის ჩამოტვირთვისას ასევე კარგი იქნება, წაიკითხოთ მიმოხილვები, რათა დარწმუნდეთ, რომ იგი უსაფრთხოა დასაინსტალირებლად და გამოსაყენებლად.

3. ხშირად განაახლეთ პროგრამული უზრუნველყოფა

პროგრამულ განახლებებს ხშირად მოყვება პატჩები, რომლებიც ასწორებენ სისტემაში სულ ბოლოს ნაპოვნ სისუსტეებს.

პროგრამული უზრუნველყოფა აგებულია კოდებზე, აპლიკაციები კი ხშირად შეიცავს კოდის ათიათასობით სტრიქონს. ჰაკერები ათვალიერებენ კოდის ყველა სტრიქონს და ხშირად პოულობენ უსაფრთხოების სისუსტეებს (იგივე „დაუცველობებს“) აპლიკაციებსა და ოპერაციულ სისტემებში. როდესაც ჰაკერები პოულობენ „დაუცველობას“, ისინი ქმნიან მავნე პროგრამას. იგი იყენებს სუსტ წერტილს თქვენს მოწყობილობაზე კონტროლის მოსაპოვებლად ან თქვენი მონაცემების მოსაპარად. საკუთარ



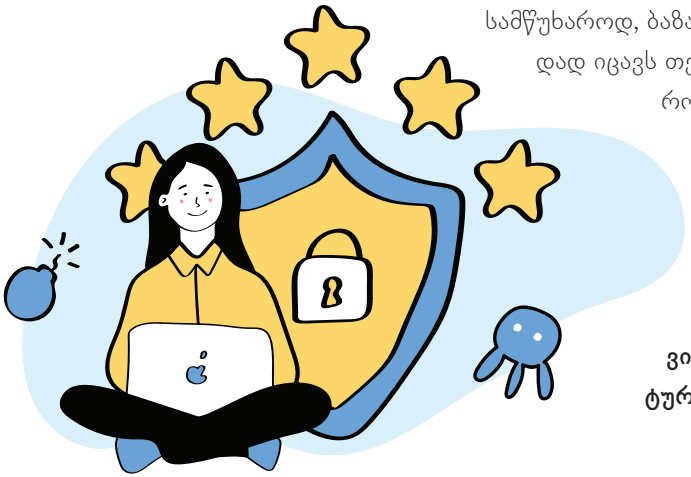
პროგრამებში დაუცველობებს დეველოპერებიც ეძებენ. პოვნისთანავე, ისინი ქმნიან პატჩებს და ავრცელებენ მათ პროგრამული უზრუნველყოფის განახლებებში. მაგრამ პატჩის დაინსტალირებამდე ჰაკერებს ამ დაუცველობის გამოყენება შეუძლიათ. ამიტომ, მნიშვნელოვანია, **პროგრამული უზრუნველყოფის განახლებები დააყენოთ გამოსვლისთანავე**.

განსაკუთრებით მნიშვნელოვანია **თქვენს კომპიუტერში ოპერაციული სისტემა და ანტივირუსული პროგრამული უზრუნველყოფა ყოველთვის განახლებული იყოს.** ავტომატურ განახლებებს თუ ჩართავთ, კომპიუტერი თავისით ჩამოტვირთავს და დააინსტალირებს კრიტიკულ პატჩებს მათი გამოშვებისთანავე. თუ სხვა აპლიკაციებისთვის ავტომატური განახლებების ჩართვა არ გინდათ, მაშინ თავად უნდა შეამოწმოთ და დააინსტალიროთ განახლებები თვეში ერთხელ მაინც.

განახლებების უმეტესობა არ დაიცავს თქვენს კომპიუტერს მანამ, სანამ არ გადატვირთავთ მას. ასე რომ, **გადატვირთეთ თქვენი მოწყობილობა, როგორც კი მოგეთხოვებათ ამის გაკეთება** განახლებების დაინსტალირების შემდეგ.

4. გამოიყენეთ სანდო ანტივირუსული პროგრამა

ანტივირუსი არ აცდის მავნე პროგრამებს დააინფიცირონ თქვენი კომპიუტერი. თუ კომპიუტერი უკვე დაინფიცირებულია, ანტივირუსი აღმოაჩენს მავნე პროგრამებს და წაშლის მათ თქვენი კომპიუტერიდან. ამიტომ, **მნიშვნელოვანია, ყოველთვის ჩართული გქონდეთ სანდო ანტივირუსული პროგრამა**. თქვენ უნდა **გაუშვათ თქვენი კომპიუტერის სრული სკანირება თვეში ერთხელ მაინც**.



სამწუხაროდ, ბაზარზე არსებული უფასო ანტივირუსების უმეტესობა ცუდად იცავს თქვენს კომპიუტერს. გამონაკლისია Microsoft Defender, რომელიც მოყვება Microsoft Windows-ის ოპერაციულ სისტემას. როდესაც კონფიგურაცია სწორად გაქვთ დაყენებული, Microsoft Defender სჯობნის ბევრ ცნობილ ანტივირუსულ პლატფორმას.

მავნე პროგრამული უზრუნველყოფა სწრაფად ვითარდება. **დარწმუნდით იმაში, რომ თქვენი ანტივირუსი განახლებულია და ვირუსების ნუსხაც ავტომატურად ახლდება**.

5. დაიცავით თქვენი კომპიუტერი პაროლით და დააყენეთ ეკრანის დამბლოკავი

ხომ არ გინდათ, რომ ვინმემ დაათვალიეროს, მოიპაროს ან წაშალოს თქვენი ფაილები, დააინსტალიროს ჯაშუშური პროგრამები ან შეცვალოს უსაფრთხოების პარამეტრები თქვენს კომპიუტერზე, როდესაც თქვენ არ ხართ მოწყობილობასთან ახლოს? **დაიცავით თქვენი კომპიუტერი ძლიერი პაროლით. დართეთ ნება კომპიუტერს, ავტომატურად დაბლოკოს თქვენი ეკრანი** უმოქმედობის ხანმოკლე პერიოდის შემდეგ.

ასევე, **დარწმუნდით, რომ გახსოვთ, როგორ დაბლოკოთ ეკრანი თქვენს მოწყობილობაზე ხელით** და არ დაგავიწყდეთ ამის გაკეთება ყოველ ჯერზე, როდესაც შორდებით მოწყობილობას.

როდესაც კომპიუტერებიდან დგებით, ხელით ეკრანის დასაბლოკად Windows 10-ზე გამოიყენეთ Win+L და Mac-ზე Command+Control+L კლავიატურის კომბინაცია. მოწყობილობასთან დაბრუნების შემდეგ კი, მოგიწევთ პაროლის ხელახლა შეყვანა.

6. გამოიყენეთ მომხმარებლის ანგარიში შეზღუდული პრივილეგიებით ყოველდღიური ამოცანებისთვის

თუ თქვენ ფლობთ კომპიუტერს, სავარაუდოდ იყენებთ მას ადმინისტრატორის ანგარიშის მეშვეობით. ეს შეიძლება ყოველთვის არ იყოს კარგი იდეა. თუ დააინსტალირებთ მავნე პროგრამით ინფიცირებულ აპლიკაციას, გახსნით ინფიცირებულ დანართს, ან დააწკაპუნებთ არასწორ ბმულზე ადმინისტრატორის ანგარიშის გამოყენებისას, ამას შეიძლება მძიმე შედეგები ჰქონდეს თქვენი მოწყობილობისათვის ან მასზე არსებული მონაცემებისთვის.

ამიტომ, კარგი იქნება შექმნათ ცალკე მომხმარებლის ანგარიში შეზღუდული პრივილეგიებით და გამოიყენოთ ის ყოველდღიური ამოცანებისთვის. ყოველთვის შეგიძლიათ შეხვიდეთ ადმინისტრატორის ანგარიშში სპეციალური ამოცანების შესასრულებლად, მაგალითად, პროგრამული უზრუნველყოფის დასაი-

ნსტალირებლად. სხვადასხვა ანგარიშების შექმნა განსაკუთრებით მნიშვნელოვანია, თუკი კომპიუტერს თქვენ გარდა სხვებიც იყენებენ.

7. დაიცავით თქვენი კომპიუტერი ფიზიკურად

თითქოს თავისთავად ცხადიცაა, მაგრამ თქვენი კომპიუტერი უნდა დაიცვათ დაკარგვისგან ან მოპარვისგან. ეს იმაზე ბევრად ხშირად ხდება, ვიდრე უმეტესობას წარმოუდგენია. არასოდეს დატოვოთ თქვენი მოწყობილობა უყურადღებოდ იქ, სადაც ის შეიძლება მოიპარონ. იფიქრეთ თქვენი კომპიუტერის სახლში დატოვებაზე, როდესაც მოგზაურობთ ან მიდიხართ იქ, სადაც შეიძლება მოგთხოვონ ციფრული მოწყობილობების დატოვება. მაგალითად, აეროპორტებში, სამთავრობო დაწესებულებებში და საელჩოებში, თუ, რა თქმა უნდა, მისი გამოყენების აუცილებლობა არ დგას. თუ ხშირად იყენებთ ლეპტოპს საჯარო ადგილას, მაგალითად, სკოლაში, საერთო სამუშაო სივრცეში, ან კაფეში, დაფიქრდით უსაფრთხოების ზომების გაზრდაზე, როგორიცაა VPN სერვისის გამოყენება.

როგორ განვაახლოთ პროგრამული უზრუნველყოფა Windows 10-ზე

თუ გსურთ, თქვენი კომპიუტერი დაიცვათ, მისი პროგრამული უზრუნველყოფა მუდმივად განახლებული უნდა იყოს. თქვენს მოწყობილობაზე ყველაზე მნიშვნელოვანი პროგრამული უზრუნველყოფა ოპერაციული სისტემაა. Microsoft-ი ხშირად აქვეყნებს Windows 10-ის განახლებებს ახალი ფუნქციებითა და უსაფრთხოების მნიშვნელოვანი პატჩებით. Windows 10-ში ავტომატური განახლებები ნაგულისხმევი პარამეტრია (ანუ ავტომატურადაა ჩართული), მაგრამ თქვენ შეგიძლიათ მართოთ, თუ როგორ და როდის დაყენდეს განახლებები.

რაც შეეხება ყველა სხვა აპლიკაციას თქვენს კომპიუტერში, ისინი აგრეთვე იღებენ მნიშვნელოვან განახლებებს. თქვენი გადასაწყვეტია, განაახლებთ მათ ხელით, თუ ოპერაციულ სისტემას ამას ავტომატურად გააკეთებინებთ. თუ პირველს აირჩევთ, მაშინ უნდა შეამოწმოთ და დააინსტალიროთ განახლებები თვეში ერთხელ მაინც.

გაითვალისწინეთ, რომ ამ ცვლილებების ჩასართავად, უნდა შეხვიდეთ თქვენს მოწყობილობაში ადმინისტრატორის ანგარიშით.

Windows 10-ზე ავტომატური განახლებების ჩართვა

იმის სანახავად, თუ რა განახლებებია უკვე მზად Windows 10-ზე დასაინსტალირებლად და აგრეთვე ავტომატური განახლებების დასაგეგმად, აირჩიეთ ღილაკი **სტარტი (Start)** და გადადით განყოფილებაში **პარამეტრები (Settings),** შემდეგ გადადით განყოფილებაში **განახლება და უსაფრთხოება (Update & Security)** და მენიუში მარცხენა მხარეს აირჩიეთ **Windows-ის განახლებათა ცენტრი (Windows Update)**.

აქ შეგიძლიათ იხილოთ ყველა მომლოდინე განახლება. Windows 10-ის ავტომატური განახლებების დასაყენებლად, გადადით ეკრანის ბოლოში და დააჭირეთ ღილაკს **დამატებითი პარამეტრები (Advanced options)**.

თქვენ შეიძლება აკრძალული გქონდეთ აქ ცვლილებების შეტანა. თუ ეს მოხდა, სავარაუდო მიზეზი არის ის, რომ თქვენი კომპიუტერი არის „Windows-დომენის“ ნაწილი. ყველაზე ხშირად ეს ნიშნავს იმას, რომ თქვენს კომპიუტერს აკონტროლებს კომპანია ან სამსახური, რომელშიც მუშაობთ.

განყოფილებაში **დამატებითი პარამეტრები (Advanced options)**, სექციის – **შეტყობინებების ჩვენება, როდესაც თქვენი კომპიუტერი განახლებების დასასრულებლად საჭიროებს გადატვირთვას (Show a notification when your PC requiresa restart to finish updating)** გასწვრივ დააჭირეთ ღილაკს **ჩართვა (On)**. შედეგად, მიიღებთ შეტყობინებას ყოველ ჯერზე, როცა კომპიუტერს დასჭირდება გადატვირთვა მნიშვნელოვანი განახლების შემდეგ.

სხვა აპლიკაციები: ჩართეთ განახლებების ავტომატური რეჟიმი ან დააინსტალირეთ ისინი ხელით.

Windows 10-ში შეგიძლიათ დააყენოთ სხვა აპლიკაციების უმეტესობა ავტომატური განახლების რეჟიმზე, Microsoft Store-ის მეშვეობით. ამისათვის დააჭირეთ ღილაკს **სტარტი (Start)** და გადადით განყოფილებაში **Microsoft Store**.

გამოსულ ფანჯარაში, ზედა პანელზე, ჩვენი მომხმარებლის სახელზე დაჭერით, გამოდის მენიუ, სადაც ავირჩევთ **აპლიკაციის პარამეტრებს** (**App Settings**), სადაც დარწმუნდებით, რომ აპლიკაციების ავტომატური განახლება ჩართულია.

როგორ განვაახლოთ პროგრამული უზრუნველყოფა MAC-ზე

ყოველწლიურად, Apple აუმჯობესებს macOS-ს ოპერაციულ სისტემას, რომელსაც იყენებთ თქვენს Mac-ზე. Apple Mac-ის ყოველწლიური განახლების ციკლს ხშირად მოაქვს განმეორებითი ცვლილებები, მაგრამ რამდენიმე წელია ის მნიშვნელოვან ცვლილებებს შეიცავს.

თქვენი macOS ოპერაციული სისტემა – ან OS X, macOS-ის ძველი ვერსიებისთვის – შეიძლება განახლდეს ყოველ შემოდგომაზე, სანამ Apple კვლავ უჭერს მხარს თქვენს მოწყობილობას. იმისათვის, რომ განვაახლოთ ოპერაციული სისტემა MAC-ზე:

- თქვენი Mac-ის მენიუს ზოლიდან აირჩიეთ **Apple-ის ხატულა ზედა მარცხენა კუთხეში** და გადადით **სისტემის პრეფერენციებზე (System Preferences)**
- აირჩიეთ **პროგრამული უზრუნველყოფის განახლება (Software Update)**

სულ ესაა, რაც უნდა გააკეთოთ. თქვენი Mac გეტყვით, არის თუ არა თქვენთვის ხელმისაწვდომი განახლება.

როგორ დავაყენოთ ან შევცვალოთ პაროლი Windows 10-ზე და Mac-ზე

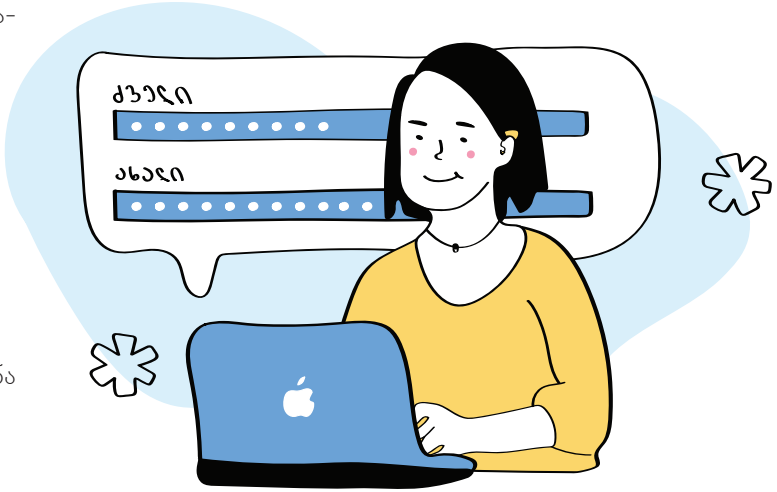
ალბათ არ გინდათ, რომ ვინმემ დაათვალიეროს თქვენი ფაილები, დააინსტალიროს ჯაშუშური პროგრამები, ან შეცვალოს უსაფრთხოების პარამეტრები თქვენს კომპიუტერზე, როდესაც ახლომახლო არ ხართ. მაშინ მიჰყევით ქვემოთ მოცემულ ინსტრუქციებს, რათა დაიცვათ თქვენი Windows 10-ის მოწყობილობა პაროლით, ან შეცვალოთ უკვე არსებული.

გაითვალისწინეთ, რომ ამ ცვლილებების განსახორციელებლად, უნდა შეხვიდეთ თქვენს კომპიუტერში ადმინისტრატორის ანგარიშით.

დააყენეთ პაროლი მოწყობილობაზე

თუ Windows 10-ზე პაროლი ჯერ არ გიყენიათ, მიჰყევით ამ ნაბიჯებს.

1. დააწკაპუნეთ ღილაკზე **სტარტი (Start)** თქვენი ეკრანის ქვედა მარცხენა მხარეს და გადადით განყოფილებაში **პარამეტრები (Settings)**.
2. გადადით განყოფილებაში **ანგარიშები (Accounts)**.
3. მენიუში მარცხნივ აირჩიეთ **შესვლის ვარიანტები (Sign-in Options)**.
4. აირჩიეთ **პაროლი (Password)** თქვენთვის ხელმისაწვდომი შესვლის ვარიანტების სიიდან და დააწკაპუნეთ ღილაკზე **დამატება (Add)**.
5. შეიყვანეთ პაროლი ველში, დაადასტურეთ და დააწკაპუნეთ ღილაკზე **შემდეგი (Next)**. დარწმუნდით, რომ პაროლი ძლიერია და მე-2 თავში მოცემული რჩევების გათვალისწინებით არის შედგენილი.
6. დააწკაპუნეთ ღილაკზე **დასრულება (Finish)**. აგრეთვე, დარწმუნდით იმაში, რომ არ დაგავიწყდათ და გახადეთ პაროლის შეყვანა



აუცილებელი პირობა თქვენს მოწყობილობაში შესასვლელად ყველასათვის, ვინც თქვენთან ერთად სარგებლობს თქვენი კომპიუტერით.

შეცვალეთ თქვენი მოწყობილობის პაროლი

მიჰყევით ამ ინსტრუქციებს უკვე არსებული პაროლის შესაცვლელად – მაგალითად, თუკი გსურთ პაროლის გაძლიერება.

1. გადადით შესვლის პარამეტრების მენიუში (**სტარტი** > **პარამეტრები** > **ანგარიშები** > **სისტემაში შესასვლელი პარამეტრები**) (Start > Settings > Accounts > Sign-in Options)
2. აირჩიეთ **პაროლი** (Password) თქვენთვის ხელმისაწვდომი სისტემაში შესასვლელი ვარიანტების სიიდან და დააწკაპუნეთ ღილაკზე **შეცვლა** (Change).
3. შეიყვანეთ თქვენი მიმდინარე პაროლი და დააწკაპუნეთ ღილაკზე **შემდეგი** (Next).
4. დააწკაპუნეთ ღილაკზე **დასრულება** (Finish).

გახადეთ მოწყობილობის პაროლის შეყვანა სავალდებულო.

მას შემდეგ, რაც დააყენებთ პაროლს თქვენს Windows 10-ზე, პაროლის შეყვანა უნდა გახადოთ სავალდებულო ყველასთვის, ვინც ეცდება მიიღოს წვდომა თქვენს კომპიუტერზე.

1. დააწკაპუნეთ ღილაკზე **სტარტი** (Start) თქვენი ეკრანის ქვედა მარცხენა კუთხეში და საძიებო ველში მოძებნეთ „**netplwiz**“. მთავარი შედეგი უნდა იყოს ამავე სახელწოდების პროგრამა. დააჭირეთ პროგრამას **netplwiz** მის გასახსნელად.
2. ფანჯარაში, რომელიც გაიხსნება, მონიშნეთ ველი – „**ამ კომპიუტერის გამოსაყენებლად, მომხმარებლებმა უნდა შეიყვანონ სახელი და პაროლი**“ (User must enter a username and password to use this computer).
3. დააჭირეთ ღილაკს **გამოყენება** (Apply).
4. ცვლილებები რომ ამოქმედდეს, პაროგრამა მოგთხოვთ თქვენი პაროლის შეყვანას. შემდეგ დააწკაპუნეთ ღილაკზე **OK**.

როგორ შევინარჩუნოთ ტელეფონის უსაფრთხოება

ელფოსტის, სოციალური ქსელების, მესენჯერების და სხვა ონლაინ სერვისების გარეშე ცხოვრება დღეს თითქმის შეუძლებელია. მაგრამ, ადრე თუ ინტერნეტის კაბელზე მიერთებულ დიდ კომპიუტერებს იყენებდნენ, დღეს მთელ ციფრულ ცხოვრებას ჯიბით ვატარებთ.

ინტერნეტში ყველაზე ხშირად სწორედ სმარტფონებით შევდივართ. ამიტომაც, ციფრული უსაფრთხოება იწყება ტელეფონის უსაფრთხო გამოყენებით. იგი სავსეა მნიშვნელოვანი მონაცემებით: კონტაქტებით, ელექტრონული წერილებით, ფოტოებით, ვიდეო და აუდიო ჩანაწერებით, შეტყობინებებით. ტელეფონზე ყველაზე ხშირად სოციალური ქსელების აპლიკაციები გვიყენია. ისინიც და სხვებიც აკვირდებიან ჩვენს გადაადგილებას (გეოლოკაციას).

ტელეფონს თუ არ გაუფრთხილდებით, ეს ყველაფერი ერთ დღეს შეიძლება ბოროტმოქმედების ხელში აღმოჩნდეს.

რაზე მივცეთ წვდომა აპლიკაციებს?

ნებისმიერი აპლიკაცია, რომელიც ჩვენს ტელეფონში აყენია, ითხოვს ტელეფონის სხვადასხვა ფუნქციაზე წვდომას. მაგალითად, იმისთვის, რომ მესენჯერით ვიდეო ზარის განხორციელება შეძლოთ, ამისათვის მას სჭირდება წვდომა ტელეფონის კამერასა და მიკროფონზე, რათა გადასცეს ხმა და გამოსახულება. თუ ვიყენებთ რუკას, მას სჭირდება ლოკაციის ფუნქცია იყოს ჩართული და ა.შ. ყველა აპლიკაციას თავისი მოთხოვნა აქვს. ერთდროულად რამდენიმე აპლიკაციას შეიძლება ჰქონდეს წვდომა ერთი და იგივე ფუნქციასთან.

თუმცა, სმარტფონის პარამეტრები იძლევა იმის საშუალებას, რომ კონკრეტულ აპლიკაციას შევუზღუდოთ კონკრეტული ფუნქცია. თქვენ უნდა გააკონტროლოთ, რაზე აქვთ წვდომა სხვადასხვა აპლიკაციებს. ზოგი აპლიკაცია მეტისმეტად „ცნობისმოყვარეა“. მაგალითად, თუკი თამაში მოგთხოვთ წვდომას

კონტაქტებსა და მიკროფონზე, სავარაუდოდ, სანდო ადამიანების შექმნილი არ იქნება და მათ ცუდი მიზნები ამოძრავებთ.

ახალ აპლიკაციას როცა იწერთ, მის ყველა მოთხოვნას ნუ დათანხმდებით. შეამოწმეთ ყველაფერი, რასაც თქვენგან ითხოვს და კარგად დაფიქრდით, რაზე მისცემთ მას წვდომას და რეალურად რომელი ფუნქცია სჭირდება სამუშაოდ.

როგორ ვმართოთ აპლიკაციის უფლებები Android-ზე?

პარამეტრები>აპლიკაციები>ჩამოტვირთული აპლიკაციები> აირჩიეთ აპლიკაცია, რომლის შემოწმებაც გინდათ> წვდომის უფლებები > გამორთეთ ან ჩართეთ უფლებები (Settings > Applications > Downloaded Apps > Choose the app you want to check > Permissions > Turn ON or OFF)

როგორ ვმართოთ აპლიკაციის უფლებები iPhone-ზე?

პარამეტრები>ჩამოსქროლეთ ბოლოში, აპლიკაციების სიამდე > აირჩიეთ აპლიკაცია, რომლის შემოწმებაც გსურთ > ჩართეთ ან გამორთეთ უფლებები (Settings > Scroll down to App list > Choose App you want to check > Turn ON or OFF)

როგორ წავშალოთ არასაჭირო აპები ჩვენს ტელეფონში?

რომელიმე აპლიკაციას თუ აღარ იყენებთ, მას ტყუილად ნუ გააჩერებთ. წაშალეთ ყველა აპლიკაცია, რომელსაც აღარ ენდობით, ან თავის დროზე „ყოველი შემთხვევისთვის“ გადმოწერეთ. ამგვარად თქვენს პირად ინფორმაციას ნაკლები საფრთხე დაემუქრება და ტელეფონშიც მეტი ადგილი შეგენახებათ.

დააყენეთ მხოლოდ ის აპები, რომელიც მართლა გჭირდებათ და რომელსაც ენდობით. აპის საიმედოობაში ეჭვი თუ გეპარებათ, აუცილებლად მოიძიეთ ინფორმაცია მის შესახებ.

როგორ წავშალოთ აპები ანდროიდზე?

პარამეტრები > აპლიკაციები > აირჩიეთ აპლიკაცია, რომლის წაშლასაც აპირებთ > წაშლა (Settings > Apps > Choose App you want to delete > Delete

როგორ წავშალოთ აპები iOS-ზე (Apple)?

დააჭირეთ იმ აპის ხატულას, რომლის წაშლაც გინდათ > ყველა ხატულა ამოძრავდება > მათ ზემოთ, მარცხნივ პატარა x გამოჩნდება > აპის წასაშლელად დააწკაპუნეთ x-ზე (Press the icon of the app to be deleted > all Apps will toggle > x will appear above > Press x to delete)

ტელეფონის ეკრანის დაბლოკვა

აუცილებლად დაბლოკეთ ტელეფონის ეკრანი. ნუ დაგავიწყდებათ, რომ სმარტფონი ფანჯარაა თქვენს ციფრულ ცხოვრებაში. შესაბამისად, ეკრანის დაბლოკვა არასასურველი სტუმრებისგან დაგიცავთ.

დაიცავით სმარტფონი საიმედო პაროლით. ან შეგიძლიათ, დააყენოთ ექვსნიშნა პინ-კოდი. ნუ გამოიყენებთ თქვენი დაბადების ან სხვა მნიშვნელოვან თარიღს. ეს კომბინაცია ადვილი გამოსაცნობია. ისიც გაითვალისწინეთ, რომ ოთხნიშნა პინ-კოდი და თითის ანაბეჭდი არასაიმედო დაცვაა. პატარა კომბინაციას მარტივად გამოიცნობენ, თითის სკანერზე დადება კი ვინმემ შეიძლება დაგაძალოთ.

ჩართეთ შესაბამისი პარამეტრი, რომ სმარტფონის ეკრანი მისი არგამოყენებიდან 1-2 წუთში დაიბლოკოს. უფრო მშვიდად იქნებით, ტელეფონი ბოროტმოქმედის ხელში რომც აღმოჩნდეს, ნაკლები შანსი ექნება, თქვენს მონაცემებზე წვდომა მოახერხოს.

გამორთეთ გეოლოკაცია

ინტერნეტის გარეშეც კი თქვენი სმარტფონი მაინც მუდმივად აკვირდება თქვენს ადგილმდებარეობას (გეოლოკაციას). იგივეს აკეთებს ზოგი აპლიკაციაც და შემდეგ გადასცემს ამ მონაცემებს სარეკლამო კომპანიებს.

თქვენი ტელეფონი აგროვებს ინფორმაციას თუ სად ცხოვრობთ და მუშაობთ, სად დადიხართ საყიდლებზე, სად ერთობით და ა.შ. ამიტომ, სასურველია, გამორთოთ გეოლოკაცია, როცა ის არ გჭირდებათ.

(მაგალითად, როცა არ იყენებთ რუკებს). დააკვირდით თითოეულ აპლიკაციას. თუ ფიქრობთ, რომ რომელიმეს არაფერში სჭირდება თქვენი ადგილმდებარეობის ცოდნა, ნუ მისცემთ მასზე წვდომას.

როგორ გამოვრთოთ გეოლოკაცია ანდროიდის ტელეფონზე?

პარამეტრები>პირადი მონაცემები>გეოლოკაცია>გამორთეთ გეოლოკაცია (Settings > Personal data > Geolocation > Turn off Geolocation

როგორ გამოვრთოთ გეოლოკაცია iPhone-ზე?

პარამეტრები>კონფიდენციალურობა>გეოლოკაციის სერვისები>გამორთეთ გეოლოკაციის სერვისები (Settings > Confidentiality > Geolocation services > Turn Geolocation services off)

როგორ ვიპოვოთ დაკარგული სმარტფონი

Apple-ის Find My აპლიკაცია საკმაოდ კარგი და გამოსადეგი აპლიკაციაა, რომლის მეშვეობითაც დაკარგული ან მოპარული სმარტფონის პოვნაა შესაძლებელი. Find My-ს ფუნქციები ნელ-ნელა იზრდება. ის კიდევ უფრო სასარგებლო Apple AirTags-ების გამოშვების შემდეგ გახდა.

ახლა კი, iOS 15-ის გამოსვლასთან ერთად, ის კიდევ უფრო ჭკვიანი ხდება. Find My შეძლებს იპოვოს თქვენი სმარტფონის ლოკაცია მაშინაც კი, თუ ის დაჯდება და გაითიშება.

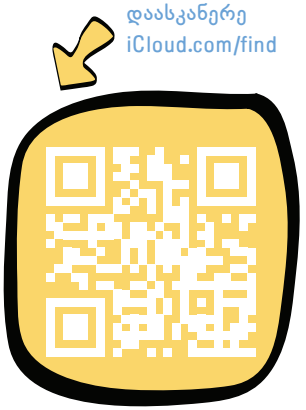
იმისათვის, რომ გათიშული სმარტფონის პოვნა შეძლოთ, სათანადო აიფონიც უნდა გქონდეთ. ეს ფუნქცია მხოლოდ უახლეს აიფონებზეა შესაძლებელი.

თუ ეს ფუნქცია ჩართული გაქვთ, თქვენი iPhone გათიშვის დროს დაგიწერთ “iPhone Findable After Power Off” – ანუ თქვენი აიფონის მოძებნა შესაძლებელია გათიშვის შემდეგაც.

როგორ გავააქტიუროთ Find My ფუნქცია?

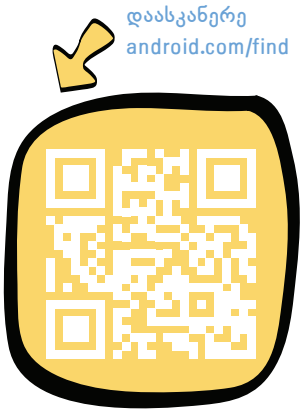
- შევდივართ Settings-ებში, შემდეგ ვაჭერთ ჩვენს სახელს
- Apple ID-ში ვაჭერთ Find My-ს
- ვრთავთ Find My iPhone-ს და თუ თქვენ iOS 15-ზე ხართ, მაშინ Find My network ფუნქციის გააქტიურებასაც შეძლებთ, რაც საშუალებას მოგცემთ, იპოვოთ თქვენი სმარტფონი გათიშულ მდგომარეობაშიც. აქვეა Send Last Location, მისი გააქტიურებით სმარტფონი გათიშვამდე გამოგიგზავნით მის ბოლო ლოკაციას.

ამის შემდეგ, თუ თქვენი სმარტფონი გაითიშება ან მოგპარავენ, თქვენ შეძლებთ ნახოთ მისი ლოკაცია Find My-ს დახმარებით Mac-დან, სხვა აიფონიდან ან ნებისმიერი ბრაუზერიდან iCloud.com/find-ზე გადასვლითა და თქვენი Apple ID-ის გამოყენებით.



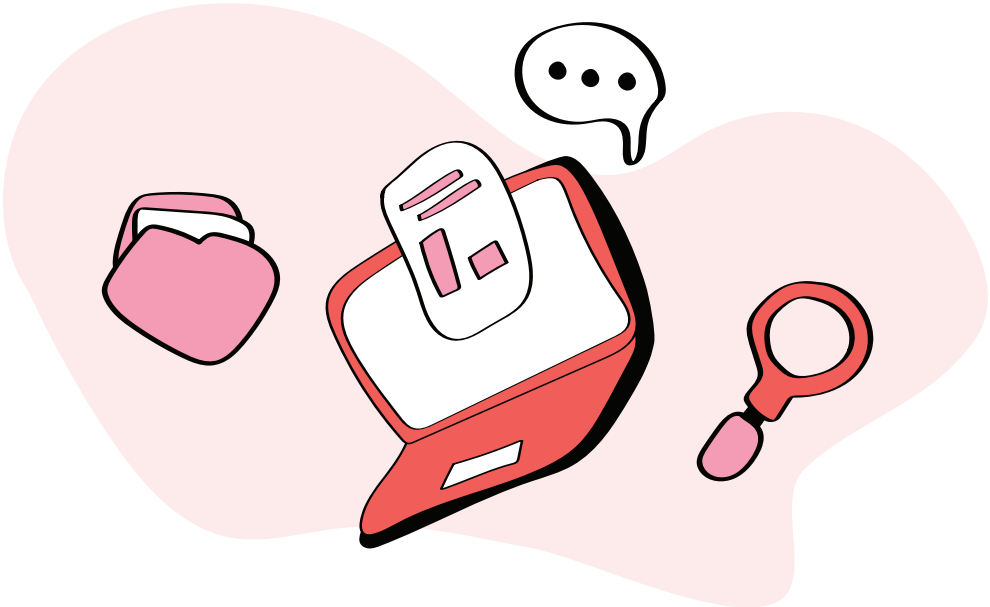
იმისათვის, რომ თქვენი Android ტელეფონის პოვნა შეძლოთ, მასში გააქტიურებული უნდა გქონდეთ Find My Device ფუნქცია (პარამეტრები > უსაფრთხოება > იპოვე ჩემი მოწყობილობა – Settings > Security > Find My Device).

დაკარგვის ან მოპარვის შემთხვევაში, ეწვიეთ გვერდს android.com/find და შეიყვანეთ თქვენი Google-ის პარამეტრები, სადაც თქვენი ტელეფონი გამოჩნდება. თქვენ შესაძლებლობა გექნებათ, დარეკოთ დაკარგულ ტელეფონზე, დაბლოკოთ ის ან წაშალოთ მასზე არსებული პროგრამული უზრუნველყოფა და ფაილები.



თავი 4. მონაცემები

პირადი მიმოწერით დაწყებული, კონფიდენციალური სამუშაო ფაილებით დამთავრებული ვქმნით და ვინახავთ ძალიან ბევრ ღირებულ და სენსიტიურ მონაცემს. მათმა დაკარგვამ შეიძლება დააზიანოს თქვენი რეპუტაცია. მეტიც, შესაძლოა მოგიხდეთ სერიოზული ფინანსური, სამართლებრივი და ადმინისტრაციული საფასურის გადახდა. მნიშვნელოვანი და სენსიტიური მონაცემების დაცვა არასასურველი წვდომისგან, მოპარვისგან, ან დაზიანებისგან,ციფრული უსაფრთხოების მნიშვნელოვანი ნაწილია.



ციფრული მონაცემები: რა არის და როდის ხდება ის პირადი

ციფრული მონაცემები ჩვენს ირგვლივაა. ყოველ ჯერზე, როცა უყურებთ ვიდეოს, კითხულობთ რაღაცას ონლაინ, ან მოგდით შეტყობინება ელფოსტაზე, მოიხმართ სხვების მიერ შექმნილ მონაცემებს. ყოველ ჯერზე, როდესაც ვინმეს წერთ, დოკუმენტში მუშაობთ, ან აქვეყნებთ რამეს სოციალურ ქსელში, თავად ქმნით საკუთარ მონაცემებს.

სამყაროში, სადაც ლამის ყველაფერი ერთმანეთს უკავშირდება, ეს მონაცემები ძალიან ღირებულია. ამ მონაცემებს აგროვებენ, აანალიზებენ და სხვადასხვა მიზნებისთვის იყენებენ. მაგალითად იმისთვის, რომ მოგყიდონ ათასი წვრილმანი, ან მოგპარონ ფული. თქვენთვის ღირებული მონაცემები რომ დაიცვათ, უნდა გაერკვეთ, რა არის მონაცემები, მათ როგორ ქმნით და შლით და ვის უნდა მათი ხელში ჩაგდება.

რა არის ციფრული მონაცემები?

ციფრული არის ნებისმიერი ინფორმაცია, რომელიც დამუშავებულია, ან შენახულია კომპიუტერზე, სმარტფონზე, თუ მეხსიერების ბარათზე. თქვენ ქმნით და მოიხმართ ამ ინფორმაციას ტექსტური დოკუმენტების, ვიდეოების, აუდიო ფაილების, სურათების, პროგრამული უზრუნველყოფის სახით და ა.შ. თუმცა, საკითხს ბოლომდე თუ გავამარტივებთ, ყველა ეს მონაცემი შედგება ერთიანებისა და ნოლებისაგან. იგივე ბინარული მონაცემებისგან.

ყველა კომპიუტერი და სმარტფონი ამ ფორმატს იყენებს, ამიტომაც ციფრული მონაცემების შექმნა, დამუშავება და შენახვა შესაძლებელია ნებისმიერ მსგავს მოწყობილობაზე. ის ასევე შეიძლება გადაიცეს ერთი მოწყობილობიდან მეორეზე, ან ხელმისაწვდომი გახდეს მილიონობით სხვა მომხმარებლისთვის ინტერნეტში.

ზოგიერთი პერსონალური მონაცემის საიმედოდ შენახვა განსაკუთრებით მნიშვნელოვანია. მაგალითად, თქვენი დაბადების თარიღის, მისამართის, პასპორტის ნომრის, მართვის მოწმობის ნომრის, საბანკო ანგარიშის, სამედიცინო ისტორიის და ა. შ. ეს იდენტიფიცირებადი პერსონალური ინფორმაციაა, ანუ ნებისმიერი მონაცემი, რომლითაც თქვენი ამოცნობა შეიძლება.

ციფრული მონაცემების შექმნა

ყოველ ჯერზე, როცა იყენებთ კომპიუტერს ან მობილურს, თქვენ ქმნით მონაცემებს. ამ მონაცემების ნაწილი შეგიძლიათ მარტივად ნახოთ. მაგალითად, როდესაც ქმნით ახალ Word-ის დოკუმენტს, აქვეყნებთ რაღაცას სოციალურ მედიაში, ან იღებთ სურათს მობილური ტელეფონით.

გაცილებით რთული სანახავია იმ მონაცემების უდიდესი ნაწილი, რომელსაც ყოველ ჯერზე, ციფრული მოწყობილობის გამოყენებით ქმნით. მაგალითად, თქვენი კომპიუტერი ინახავს დეტალურ ჩანაწერებს, დროის რა მონაკვეთში იყენებთ მას და კონკრეტულ აპლიკაციებს. თქვენი ინტერნეტ ბრაუზერი აკვირდება, რომელ ვებგვერდებზე შედიხართ, თითოეულზე რამდენ დროს ატარებთ, იქ რაზე აწკაპუნებთ და იქიდან რას იწერთ. ფოტოს ყველა გადაღებაზე, სმარტფონი იმახსოვრებს, სად და როდის მოხდა ეს. თუ ზუსტად არ იცით, სად უნდა ეძებოთ, ამ მონაცემებს ვერ დაინახავთ.

ციფრული მონაცემების წაშლა

მონაცემების წაშლა არც ისე ადვილია. „წაშლაზე“ დაწკაპუნებით, ფაილს აგდებთ სანაგვე კალათაში. იქ ოპერაციული სისტემა მას რაღაც დროით შეინახავს. ამ ფაილს მარტივად იპოვის ყველა, ვისაც ექნება წვდომა თქვენს მოწყობილობაზე.

მაგრამ მაშინაც კი, თუ თქვენ ასუფთავებთ სანაგვე კალათას ან შლით ფაილებს მისი გვერდის ავლით, ისინი მაინც არ ქრება თქვენი მოწყობილობიდან. როდესაც წაშლით ფაილებს, მოწყობილობის ოპერაციული სისტემა იღებს სიგნალს, რომ ეს ფაილები აღარ გჭირდებათ და წყვეტს მათ ჩვენებას. სინამდვილეში ოპერაციული სისტემა არ აქრობს ამ ფაილებს. იმ სივრცეს, რომელსაც ძველი ფაილები იკავებდნენ მოწყობილობის მყარ დისკზე, იგი მონიშნავს, როგორც ხელმისაწვდომს. მხოლოდ მაშინღა, როდესაც ეს სივრცე სხვა რამისთვის გახდება საჭირო, ოპერაციული სისტემა წაშლილი ფაილების ბინარულ მონაცემებს ზემოდან ახალს გადააწერს. ეს სანამ მოხდება, „წაშლილი“ ფაილები რჩება თქვენს მოწყობილობაზე. მათი აღდგენა არც ისე რთულია.

დაასკანერე BleachBit

არსებობს სპეციალური ხელსაწყოები, რომლითაც შეძლებთ, საიმედოდ გაანადგუროთ ფაილები თქვენს მოწყობილობაზე. ანუ წაშალოთ ისინი და შეცვალოთ მათი ბინარული მონაცემები ერთებისა და ნულების შემთხვევითი კომბინაციებით. იმისათვის, რომ ფაილები ისე წაშალოთ მოწყობილობიდან, რომ მათი აღდგენა შეუძლებელი

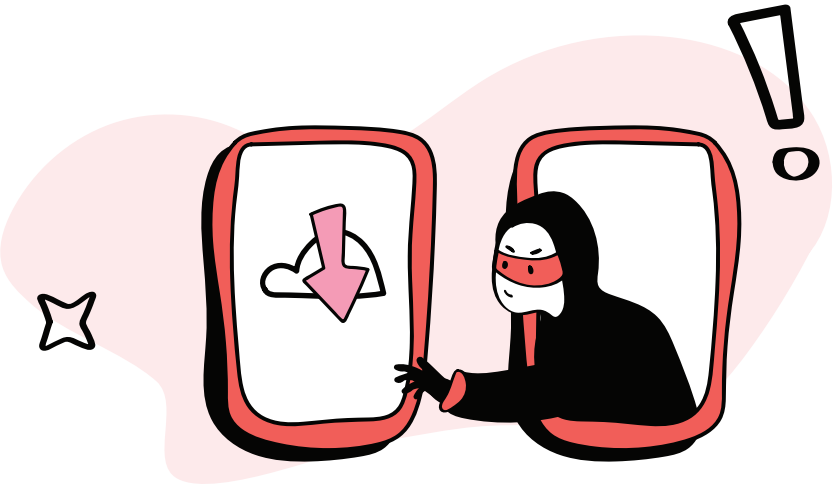
გახდეს, გამოიყენეთ პროგრამა BleachBit. ის უფასო ინსტრუმენტია, რომელიც საიმედოდ და სამუდამოდ წაშლის მონაცემებს თქვენი მყარი დისკიდან.

ინტერნეტში გაზიარებული მონაცემების წაშლა გაცილებით რთულია. ფოტოების სოციალურ ქსელში გამოქვეყნებისას, ელფოსტით სხვადასხვა სერვისებზე რეგისტრაციისას, შეტყობინებების აპლიკაციების საშუალებით დოკუმენტების გაზიარებისას, ვიდეოებს ფაილების გამაზიარებელი საიტებით გაგზავნისას, ყოველთვის ვერ გააკონტროლებთ, თუ ვის ექნება ამ მონაცემების ასლები.

ვის უნდა თქვენი მონაცემების ხელში ჩაგდება?

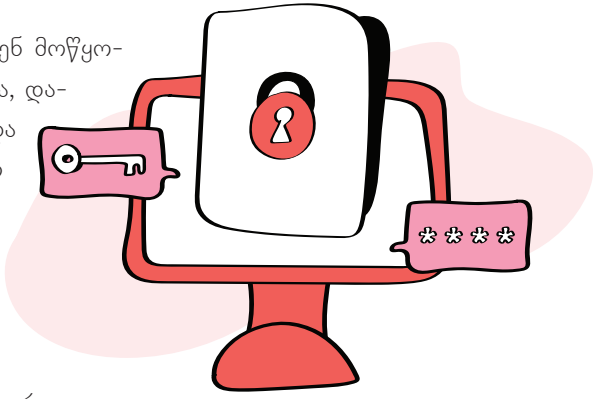
ზუსტად არასოდეს იცით, ვის დააინტერესებს თქვენს მოწყობილობებზე არსებული მონაცემები. ინდივიდებს, ჯგუფებს ან ორგანიზაციებს თქვენს მონაცემებზე წვდომა სხვადასხვა მიზნით შეიძლება უნდოდეთ. მაგალითად, საბანკო მონაცემების, ან ფოტოებისა და ვიდეოების მოსაპარად, რათა შემდეგ დაგაშანტაჟონ. რადგან ზუსტად იცით, ვინ და რატომ შეიძლება დაინტერესდეს თქვენი ინფორმაციით, ყოველთვის იზრუნეთ, რომ თქვენი კომპიუტერი, მობილური და ფაილების შესანახი მოწყობილობები საიმედოდ იყოს დაცული.

გარდა ამისა, უამრავ ინფორმაციას ტოვებთ ინტერნეტში კომპიუტერის ან მობილურის გამოყენებისას. დარწმუნდით, რომ გესმით რა სახის ინფორმაციას ავრცელებთ ონლაინ ყოფნისას, როგორ ხდება ამ ინფორმაციის გამოყენება და რისი გაკეთება შეგიძლიათ თქვენი ონლაინ კვალის შესამცირებლად.



როგორ გავუფრთხილდეთ მონაცემებს ჩვენს მოწყობილობაზე

იმ ციფრულ მოწყობილობებზე, რომელსაც სამსახურისთვის და პირადი საქმეებისთვის იყენებთ, თქვენი ძალიან ბევრი მონაცემი ინახება. თქვენი ლეპტოპი, მობილური ტელეფონი, ტაბლეტი, გარე მყარი დისკი და ყველა ახლომდებარე USB დისკი ინახავს მონაცემებს ტექსტური დოკუმენტების, სურათების, ვიდეოების, აუდიო ჩანაწერების და სხვა სახით. ამ მოწყობილობებზე შეიძლება ინახებოდეს ის ფაილებიც, რომელიც წაშლილი გგონიათ.



რა მოხდება, თუ ვინმე თქვენს ფაილებს დაეუფლება, მოიპარავენ მოწყობილობას, რომელზეც თქვენი პირადი ან პროფესიული ფაილებია, დაკარგავთ ასეთ მოწყობილობას, ან მოწყობილობა დაზიანდება და თქვენ დაკარგავთ ყველა მნიშვნელოვან ინფორმაციას? მიჰყევით ამ რჩევებს, თქვენთვის ღირებული მონაცემების დასაცავად.

1. ფიზიკურად დაიცავით თქვენი მოწყობილობები

ეს თითქოს თავისთავად ცხადია, მაგრამ თქვენი ციფრული მონაცემების დასაცავად, ერთ-ერთი საუკეთესო გზა მოწყობილობის გაფრთხილებაა. ლეპტოპი, მობილური ტელეფონი, ტაბლები, მყარი დისკი, მეხსიერების ბარათი შეიძლება დაკარგოთ, ან მოგპარონ. ეს თუ მოხდა, მოწყობილობის მპოვნელს წვდომა ექნება ყველა იმ პირად მონაცემზე, რომელსაც შიგნით ინახავთ.

ამიტომაც, თუ თქვენს მოწყობილობას არ იყენებთ, შეინახეთ იგი უსაფრთხო და დაცულ ადგილას. ყურადღება მიაქციეთ გარე მეხსიერების ყველა მოწყობილობას, რომელსაც იყენებთ, მათ შორის მყარ დისკებს, მიკროჩიპებს, USB მეხსიერების ბარათებს, ან რეტროს მოყვარული თუ ხართ, CD-ებსა და DVD-ებსაც. შეინახეთ ისინი დაცულ ადგილას. ისეთ ადგილებში, სადაც მოწყობილობა შეიძლება მოგპარონ, უყურადღებოდ არ დატოვოთ. მოგზაურობისას ან ისეთი ადგილის სტუმრობისას, სადაც მოგეთხოვებათ თქვენი ციფრული მოწყობილობების ჩაბარება (მაგალითად: აეროპორტები, სამთავრობო ოფისები და საელჩოები), დაფიქრდით, ხომ არ აჯობებს ისინი სახლში დატოვოთ? თუ ხშირად იყენებთ ლეპტოპს

ნახევრად საჯარო ადგილებში, მაგალითად, სკოლებში, საერთო სამუშაო სივრცეებში, ან კაფეებში, გირჩევთ, კენსინგტონის კაბელი იყიდოთ.

2. დაიცავით თქვენი მოწყობილობები პაროლით

თუ თქვენს ციფრულ მოწყობილობებს ძლიერი პაროლებით დაიცავთ, უფრო გაურთულებთ საქმეს მას, ვინც თქვენი პირადი მონაცემებით დაინტერესდება. მოწყობილობის დაკარგვის, ან მოპარვის შემთხვევაში, ასე მონაცემებსაც იცავთ, თუმცა არა სრულად.

ყველა მოწყობილობაზე ჩართეთ ეკრანის ავტომატური დაბლოკვა ხანმოკლე უმოქმედობის შემდეგ. დარწმუნდით, რომ იცით, როგორ უნდა დაბლოკოთ ეკრანი თქვენს მოწყობილობაზე და გააკეთეთ ეს ყოველ ჯერზე, როცა ტოვებთ მას.

3. დაშიფრეთ სენსიტიური ფაილები

თქვენს მოწყობილობებზე სენსიტიური მონაცემების დასაცავად საუკეთესო გზა მათი დაშიფვრაა. ეს მოწყობილობაზე არსებულ ყველა მონაცემს სრულიად წაუკითხავს ხდის. დაშიფრული მონაცემების წაკითხვა შეუძლია მხოლოდ მას, ვისაც აქვს პაროლი, ან გაშიფვრის გასაღები.

4. შექმენით მონაცემების სარეზერვო ასლი

მოწყობილობა თუ სხვას ჩაუვარდა ხელში, შეიძლება ნახონ ის, რაც არ გინდათ, რომ სხვებმა ნახონ. მაგრამ ეს ერთადერთი რისკი არაა. თქვენ ასევე რისკავთ, დაკარგოთ წვდომა მნიშვნელოვან ფაილებზე, რომელთა ნაწილსაც ვერასდროს შეცვლით. მონაცემებს ასევე დაკარგავთ, თუ მოწყობილობა მწყობრიდან გამოვა, ან მავნე პროგრამის შეტევის შემდეგ დაიშიფრება.

ფაილების დაკარგვისგან თავი რომ დაიზღვიოთ, ამისთვის შექმენით თქვენი მონაცემების სარეზერვო ასლები. თუ ამაზე ხშირად ფიქრი დამღლელია თქვენთვის, თქვენს მოწყობილობას შეუძლია ეს ავტომატურად გააკეთოს ხოლმე.

5. გამოიყენეთ ანტივირუსული პროგრამა და განაახლეთ თქვენი სისტემა

კარგი ანტივირუსული პროგრამა დაიცავს თქვენს მოწყობილობებს მავნე პროგრამებისგან, რომლებსაც შეუძლიათ მოგპარონ მონაცემები, დააზიანონ, ან გაანადგურონ ისინი. დარწმუნდით, რომ იყენებთ ლიცენზირებულ ანტივირუსულ პროგრამას. თუ Windows-ის მომხმარებელი ხართ, თქვენს ოპერაციულ სისტემაში ჩაშენებულია ეფექტური ანტივირუსი – Microsoft Defender.

დარწმუნდით, რომ თქვენი ანტივირუსული პროგრამა და ოპერაციული სისტემა განახლებულია. გირჩევთ, ეს პროგრამა დააყენოთ ავტომატურად განახლების რეჟიმზე.

6. ფაილების უსაფრთხოდ წაშლა

ფაილების წაშლა თქვენს კომპიუტერზე, მობილურ მოწყობილობაზე ან გარე მეხსიერების მოწყობილობაზე რეალურად არ ნიშნავს ფაილების გაქრობას. მონაცემები რჩება მოწყობილობაზე და შესაძლებელია მისი აღდგენა. ერთადერთი გზა თქვენი ფაილების სამუდამოდ წაშლის უზრუნველსაყოფად არის სპეციალური პროგრამული უზრუნველყოფის გამოყენება, რომელიც გადაწერს წაშლილ მონაცემებს შემთხვევითი კოდით. თუ გაკეთებული გაქვთ თქვენი მონაცემების სარეზერვო ასლები, გახსოვდეთ, რომ მოწყობილობებიდან მგრძნობიარე ფაილების წაშლა არ შლის ასლებს.

დაასკანერე BleachBit

BleachBit უფასო და ღია წყაროზე დაფუძნებული ინსტრუმენტია, რომელიც შეგიძლიათ გამოიყენოთ ტრადიციული მყარი დისკებიდან მონაცემების უსაფრთხოდ და სამუდამოდ წასაშლელად. თუ იყენებთ SSD დისკებს (ასევე ცნობილია როგორც ფლეშ დრაივები), სამწუხაროდ, მონაცემების უკვალოდ წაშლას ყოველთვის ვერ მოახერხებთ.

7. უსაფრთხოდ გადაყარეთ ძველი მოწყობილობები

თქვენი ძველი კომპიუტერის, მობილურის ან სხვა შესანახი მოწყობილობის გაყიდვამდე, გადამუშავებამდე ან გადაგდებამდე, დარწმუნდით, რომ არ ტოვებთ მასზე რაიმე პერსონალურ ან კონფიდენციალურ ინფორმაციას. გაასუფთავეთ თქვენი მოწყობილობა სანდო ხელსაწყოს გამოყენებით, რათა უსაფრთხოდ და სამუდამოდ წაშალოთ მონაცემები და დააბრუნოთ იგი ქარხნულ პარამეტრებზე.

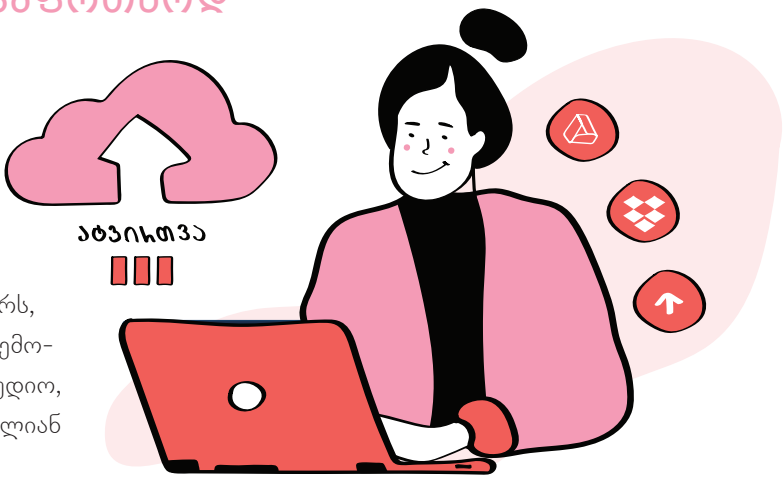
თუ თქვენ ყრით ძველ CD-ებს, DVD-ებს, SSD-ის შესანახ მოწყობილობებს, USB დისკებს ან სხვა შესანახ მოწყობილობას, აჯობებს ისინი ფიზიკურად გაანადგუროთ, ჩაქუჩის, ან სხვა ხელსაწყოების გამოყენებით.

8. არ გააზიაროთ კონფიდენციალური მონაცემები

საჯარო სამსახურის ან თქვენი პირადი სენსიტიური ან კონფიდენციალური მონაცემების დასაცავად საუკეთესო გზაა, ისინი არავის გაუზიაროთ. როცა ციფრულ ფაილებს სხვებს უზიარებთ, ამ მონაცემების უსაფრთხოებაზე სრული კონტროლი აღარ გაქვთ.

როგორ შევინახოთ და გავაზიაროთ ფაილები ონლაინ უსაფრთხოდ

იქნება ეს პირადი თუ პროფესიული ფაილი, ყველა მნიშვნელოვანია. მაგრამ, ზოგი ფაილი მაინც უფრო მნიშვნელოვანია, ვიდრე სხვები. გაუფრთხილდით ნებისმიერ ფაილს, რომელიც შეიცავს: თქვენი დაბადების თარიღს, მისამართს, პასპორტის ნომერს, მართვის მოწმობის ნომერს, საბანკო ანგარიშს, სამედიცინო ჩანაწერებს, საშემოსავლო გადასახადის ჩანაწერებს და ა. შ. ზოგი აუდიო, ფოტო და ვიდეო ფაილი ასევე შეიძლება იყოს ძალიან პირადი და მნიშვნელოვანი.



ასეთი მონაცემები თქვენს მოწყობილობაში საიმედოდ უნდა შეინახოთ, მაგრამ არსებობს კიდევ ერთ გზა მათ დასაცავად – არასდროს ატვირთოთ ან გამოაქვეყნოთ ისინი ინტერნეტში. **არავის გაუზიაროთ ძალიან პირადი ან სენსიტიური ფაილები ინტერნეტში, აუცილებელი შემთხვევების გარდა**. სანამ მონაცემები თქვენს მოწყობილობაზეა, მათ უსაფრთხოებას თითქმის სრულად აკონტროლებთ. მაგრამ კონტროლი ქრება, როგორც კი მათ ინტერნეტში ატვირთავთ, ან ვინმეს გაუზიარებთ.

თუ გადაწყვიტეთ ფაილების შენახვა ან ინტერნეტში გაზიარება, მნიშვნელოვანია, გქონდეთ შესაბამისი ცოდნა და ეს უსაფრთხოდ გააკეთოთ.

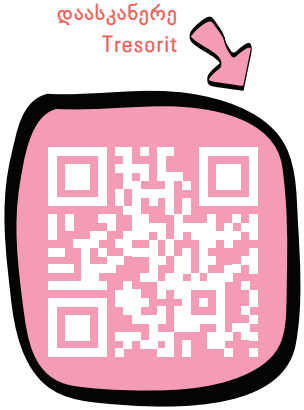
ფაილების ონლაინ უსაფრთხოდ შენახვა

Dropbox, Google Drive, OneDrive, Tresorit – ფაილების ღრუბელზე შესანახად უამრავი სერვისი არსებობს. ამ სერვისების წყალობით, მარტივად გექნებათ წვდომა თქვენს ფაილებზე ნებისმიერი მოწყობილობიდან, ნებისმიერ ადგილას. ასევე, მათი საშუალებით, შეგიძლიათ სხვა ადამიანებსაც მისცეთ წვდომა თქვენს ფაილებზე და ზოგიერთზე ერთად იმუშაოთ კიდეც.

ფაილების საცავებში თქვენი მონაცემების საიმედოდ დასაცავად მიჰყევით შემდეგ ნაბიჯებს:

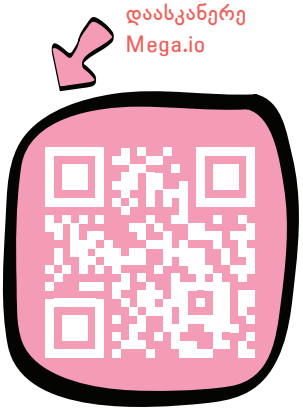
- გამოიყენეთ სანდო სერვისი და დარწმუნდით, რომ ის დაშიფრავს თქვენს ფაილებს, როგორც გადაცემის დროს, ისე შენახვისას. შეძლებისდაგვარად, აირჩიეთ სერვისები, რომელიც ნულოვანი ცოდნის დაშიფვრას გთავაზობთ. მაგალითად, Tresorit და Mega.io, ეს იმისთვის, რომ თქვენი მონაცემები უსაფრთხო იქნება მაშინაც კი, თუ თქვენი ღრუბლოვანი პროვაიდერი მწყობრიდან გამოვა. მსგავს სერვისებზე თქვენი ანგარიშები უნდა დაიცვათ ძლიერი და უნიკალური პაროლებით.

დაასკანერე Tresorit



- ჩართეთ ორნაბიჯიანი ავტორიზაცია, რათა დაიცვათ თქვენი ფაილი მოწყობილობის მოპარვის ან პაროლის გატეხვის შემთხვევაში.
- თუ სხვა ადამიანებს აძლევთ თქვენს ონლაინ ფაილებზე წვდომის უფლებას, დარწმუნდით, რომ ისინი ასევე იცავენ თავიანთ ანგარიშებს ძლიერი პაროლებითა და ორნაბიჯიანი ავტორიზაციით.
- ეცადეთ, ონლაინ არ შეინახოთ ძალიან ბევრი სენსიტიური და კონფიდენციალური ფაილი. არ ატვირთოთ მნიშვნელოვანი

დაასკანერე Mega.io



პერსონალური, ან პროფესიონალური ფაილები ერთზე მეტ სერვისზე. წაშალეთ ეს ფაილები, როდესაც მიხვდებით, რომ ისინი ონლაინ სივრცეში აღარ დაგჭირდებათ.

ფაილების უსაფრთხოდ გაზიარება

თუ სენსიტიური ან კონფიდენციალური ფაილის გაგზავნა გჭირდებათ, ამის გასაკეთებლად რამდენიმე მარტივი გზა არსებობს. რომელი ხერხიც არ უნდა აირჩიოთ, გაერკვიეთ, იმ რისკებში რომელიც ამ ხერხით მონაცემების გაზიარებას ახლავს თან. დააზუსტეთ, როგორ შეგიძლიათ მათი შემცირება.

- **ფაილის გაზიარების სერვისები**

ფაილების გაზიარება შესაძლებელია ონლაინ საცავში, ან ფაილების გაზიარების სერვისში ატვირთვით, ან ვინმესთვის ამ ფაილების ბმულის გაგზავნით. თუ ამ მეთოდს აირჩევთ, აუცილებლად გაითვალისწინეთ ზემოთ ჩამოთვლილი სიფრთხილის ზომები. ასევე, თქვენ მიერ შექმნილ გაზიარების ბმულებს უნდა მოეპყროთ, როგორც პირად, სენსიტიურ მონაცემებს.

დაასკანერე ProtonMail

- **ელფოსტა**

კონფიდენციალური ფაილების გასაგზავნად შეგიძლიათ გამოიყენოთ ელფოსტაც. უსაფრთხოებისთვის მიიღეთ შემდეგი ზომები:

- გამოიყენეთ უსაფრთხო და დაშიფრული ელფოსტის სერვისი. ProtonMail და Tutanota გთავაზობთ უფასო, ღია წყაროზე დაფუძნებულ, სრული დაშიფვრის ელფოსტის სერვისს.
- დაიცავით თქვენი ელფოსტის ანგარიში ძლიერი და უნიკალური პაროლით.
- ჩართეთ ორნაბიჯიანი ავტორიზაცია თქვენი ელფოსტის ანგარიშზე.
- დარწმუნდით, რომ ადამიანებს, რომლებსაც უგზავნით სხვადასხვა ფაილებს, დაცული აქვთ მათი ანგარიშები ძლიერი პაროლითა და ორფაქტორიანი ავტორიზაციით.
- მას შემდეგ, რაც დარწმუნდებით, რომ ადრესატმა თქვენი ფაილები მიიღო, წაშალეთ ისინი თქვენი ელფოსტის ანგარიშიდან. არ დაგავიწყდეთ მათი წაშლა ელფოსტის ურნიდანაც.

დაასკანერე Tutanota

- **შეტყობინებების აპლიკაციები**

ასევე, შეგიძლიათ გამოიყენოთ შეტყობინებების აპლიკაციები ნაკლებად კონფიდენციალური, მაგრამ მგრძნობიარე ინფორმაციის გასაზიარებლად. ეს აპლიკაციები იდეალუ-

რია პირადი სურათებისა და ვიდეოების გასაზიარებლად. თუ ამას აკეთებთ, დარწმუნდით, რომ იყენებთ სანდო, ბოლომდე დაშიფრულ შეტყობინებების აპლიკაციას, მაგალითად, Signal-ს ან Wire-ს. თქვენ შეგიძლიათ გამოიყენოთ გაუჩინარებადი შეტყობინებები, რათა ისინი აპლიკაციაში არ დარჩეს.

რატომ უნდა გააკეთოთ სარეზერვო ასლები და სად უნდა შეინახოთ ისინი

მნიშვნელოვანი მონაცემების დაკარგვა ბევრად უფრო ადვილია, ვიდრე გგონიათ. ეს ყველაზე ხშირად ხდება მომხმარებლის შეცდომის, ტექნიკის გაუმართაობის, მოწყობილობის მოპარვის, ან დაკარგვის და მავნე პროგრამის „წყალობით“. თქვენს მოწყობილობებზე არსებული ფაილებისთვის, მნიშვნელოვან რისკებს წარმოადგენს ე. წ. „რენსომვეარები“ (Ransomware) და ჰაკერული შეტევები.

მნიშვნელოვანი ფაილების ყველა ამ რისკისგან დასაცავად, ერთადერთი გზაა ხშირად შექმნათ თქვენი მონაცემების სარეზერვო ასლები. ისინი უნდა შეინახოთ მყარ დისკზე, გარე მეხსიერების მოწყობილობაზე, ან ღრუბელოვან სერვისზე. მონაცემთა სარეზერვო ასლების წყალობით, სწრაფად აღადგენთ მნიშვნელოვან ფაილებს თქვენს მოწყობილობებზე, დედანის დაკარგვის ან დაზიანების შემთხვევაში.

სად უნდა შეინახოთ თქვენი სარეზერვო ასლები

თქვენი მონაცემების სარეზერვო ასლის შესანახად, შეგიძლიათ გამოიყენოთ თქვენი მოწყობილობის მყარი დისკი, გარე მეხსიერების მოწყობილობა, ან ღრუბელი. თითოეულ ამ ვარიანტს აქვს დადებითი და უარყოფითი მხარეები.

ლოკალური მყარი დისკი

ყველაზე მოსახერხებელი სარეზერვო დანიშნულების ადგილი არის თქვენი მოწყობილობის მყარი დისკი. თქვენ შეგიძლიათ შექმნათ დისკზე ცალკე დანაყოფი და იქ შეინახოთ სარეზერვო ასლები. ლოკალურ მყარ დისკზე მონაცემთა სარეზერვო ასლის შენახვის ყველაზე დიდი მინუსი ისაა, რომ ის ვერ გიცავთ მყარი დისკის სრული დაზიანების, მავნე პროგრამის და თქვენი მოწყობილობის დაკარგვის ან მოპარვისგან.

გარე მეხსიერების მოწყობილობა

მხოლოდ მოწყობილობის იმედად რომ აღარ იყოთ, გამოიყენეთ გარე მყარი დისკები ან USB მეხსიერების ბარათი. მეხსიერების პორტატულ მოწყობილობაზე ბევრი მონაცემის შენახვა შეიძლება. თუ მათ დაშიფრავთ, ეს ძალიან საიმედოა. მათი გამოყენება არის უფრო მარტივი, სწრაფი და იაფი, ვიდრე დისტანციური სარეზერვო ასლების შექმნა.

თუმცა, ეს შესანახი მოწყობილობები დაუცველია ისეთი ბუნებრივი კატასტროფების წინააღმდეგ, როგორიცაა წყალდიდობა და ხანძარი. მავნე პროგრამას შეუძლია თქვენს მთავარ დისკთან ერთად დააინფიციროს ეს მოწყობილობები. ასევე, შეიძლება დაიკარგოს ან მოიპაროს.

Cloud-ის მეხსიერების სერვისი

მონაცემთა სარეზერვო ასლების შესაქმნელად, ღრუბლის გამოყენება სულ უფრო პოპულარული ხდება. ღრუბლოვანი სერვისების უმეტესობა გთავაზობთ დიდ ადგილს მეხსიერებისთვის და მონაცემთა დაშიფვრას. იქ ატვირთულ მონაცემებზე ნებისმიერ დროს გექნებათ წვდომა და შეძლებთ, მართოთ თქვენი მონაცემები ნებისმიერი დაკავშირებული მოწყობილობით.

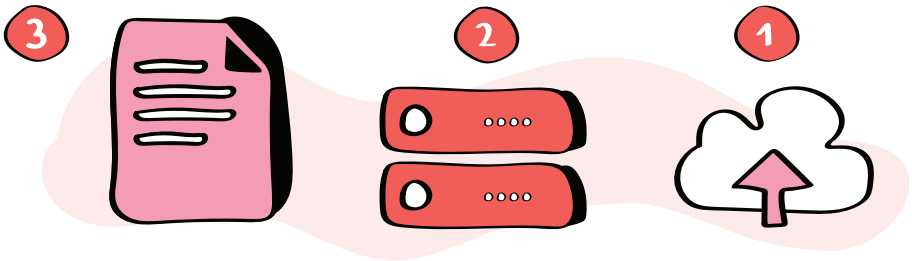
ასე მონაცემებზე ნერვიულობა აღარ მოგიწევთ, რადგან სარეზერვო ასლები იქნება შენახული შორს და საიმედოდ. გეცოდინებათ, რომ რამე თუ მოხდება, მარტივად აღადგენთ მათ. გარდა ამისა, ღრუბელზე შეგიძლიათ შეინახოთ ფაილის მრავალი ვერსია. ანუ, თუ დაგჭირდათ, ძველ ვერსიებსაც აღადგენთ. თუმცა, ღრუბლოვანი სერვისები უფრო ნელი და ხშირად უფრო ძვირია, ვიდრე ფაილების „ადგილობრივი“ დარეზერვება. თანაც, ღრუბელზე შენახულ მონაცემებზე წვდომა ვერ გექნებათ ინტერნეტის გარეშე.

ღრუბლის შერჩევისას, მიანიჭეთ უპირატესობა მათ, ვინც დაშიფრულ მეხსიერებასთან ერთად გთავაზობთ ე.წ. „ნულოვან ცოდნას“, რაც იმას ნიშნავს, რომ შემნახველი კომპანიაც კი შეძლებს თქვენი ფაილების ნახვას. როგორც ჩვეულებრივ, ისე დაშიფრულ, „ნულოვანი ცოდნის“ ღრუბლებზე ფაილების ატვირთვა შეგიძლიათ უფასოდ.

რომელ ღრუბელსაც არ უნდა იყენებდეთ, დარწმუნდით, რომ თქვენს ანგარიშს იცავთ ძლიერი და უნიკალური პაროლით და ჩართული გაქვთ ორნაბიჯიანი ავტორიზაცია.

„წესი 3-2-1“ მნიშვნელოვანი მონაცემების სარეზერვო ასლის შესაქმნელად

შეიძლება გქონდეთ ფაილები, რომლებიც თქვენთვის განსაკუთრებით მნიშვნელოვანია. კარგი იქნება, თუ ამ ფაილების სარეზერვო ასლებს ერთზე მეტ ადგილას შეინახავთ. სენსიტიური, კონფიდენციალური ან ღირებული მონაცემების დასაცავად, მიჰყევით სარეზერვო ასლების დაცვის „3-2-1 წესს“. ანუ, ყოველთვის შეინახეთ თქვენი მონაცემების სამი ასლი, ორი სხვადასხვა ლოკალურ მოწყობილობაზე და ერთიც დისტანციურად.



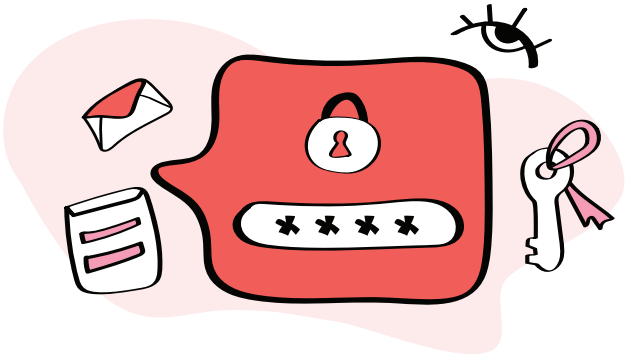
ასე გამოვა, რომ მონაცემების ორიგინალი გექნებათ თქვენს მოწყობილობაზე, ერთი სარეზერვო ასლი პორტატული მეხსიერების მოწყობილობაზე და მეორე ღრუბელზე. ეს სისტემა შეგინარჩუნებთ მონაცემებს, იმ (ნაკლებად სავარაუდო) შემთხვევაშიც კი, თუ თქვენ დაკარგავთ მის ორ ასლს ერთდროულად.

რატომ უნდა დაშიფროთ თქვენი მოწყობილობები

თქვენს კომპიუტერზე, ტაბლეტსა და სმარტფონზე ინახება ბევრი მნიშვნელოვანი და თქვენთვის მგრძნობიარე მონაცემი. მოწყობილობის დაკარგვის, ან მოპარვის შემთხვევაში, სხვას ექნება წვდომა ყველაფერზე, რაც იქ ინახება და შესაძლოა ეს დამცავმა პაროლმაც ვერ აგარიდოთ თავიდან.

თქვენს მოწყობილობებზე სენსიტიური მონაცემების დასაცავად, საუკეთესო გზა მათი დაშიფვრაა. დაშიფვრის წყალობით, მოწყობილობაზე არსებული ყველა მონაცემი სრულიად წაუკითხავი ხდება. შე-

დეგად, ისინი დაცულია უცხო პირების წვდომისა და მანიპულაციებისგან. ეს განსაკუთრებით მნიშვნელოვანია, როდესაც საქმე გაქვთ სენსიტიურ მონაცემებთან, რამაც შეიძლება საფრთხე შეგიქმნათ თქვენ, ან იმ ადამიანებს, ვისთან ერთადაც მუშაობთ.



როგორ მუშაობს დაშიფვრა?

კომპიუტერზე, სმარტფონზე ან მეხსიერების ბარათზე, დამუშავებული ან შენახული ინფორმაცია, ყველაზე საბაზისო დონეზე, შედგება ერთიანებისა და ნულების თანმიმდევრობისაგან. მას ასევე ეძახიან ბინარულ მონაცემებს. ამ ფორმატს უკლებლივ ყველა კომპიუტერი და სმარტფონი იყენებს. ამიტომაც, ციფრული მონაცემების შექმნა, დამუშავება და შენახვა შესაძლებელია ნებისმიერ მსგავს მოწყობილობაზე.

დაშიფვრა ბინარულ მონაცემებს გარდაქმნის რთულ კოდად, რომლის წაკითხვაც შეუძლიათ მხოლოდ იმ ადამიანებს, ვისაც 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.

დისკის სრული დაშიფვრა

დისკის სრული დაშიფვრა აპარატურის დონეზე შიფრავს თქვენს მოწყობილობაზე შენახულ ყველა მონაცემს. ის თქვენს მყარ დისკზე არსებულ მონაცემებს ავტომატურად გარდაქმნის რთულ, წაუკითხავ კოდად. გაშიფვრის გასაღების გარეშე, დაშიფრულ მოწყობილობაზე ფაილების წაკითხვას ვერავინ შეძლებს.

დისკის სრული დაშიფვრა მარტივია, რადგან კომპიუტერის განბლოკვის შემდეგ მეტი აღარაფრის გაკეთება არ გიწევთ. ის მუშაობს თქვენგან შეუმჩნევლად.

დისკის სრული დაშიფვრის უპირატესობა ისიცაა, რომ აღარ გჭირდებათ ფიქრი იმაზე, თუ როგორ დაიცვათ ცალკეული ფაილები. როგორც კი მონაცემებს შექმნით, ისინი ავტომატურად იშიფრება. იგივე ხდება მათი წაკითხვის შემდეგაც. დისკის სრული დაშიფვრის წყალობით, დაცულია ისეთი მონაცემებიც,

რომელთა არსებობაც ხშირად აღარ გვახსოვს (მაგალითად, დროებითი ფაილები და ბრაუზერის ქეშის ფაილები).

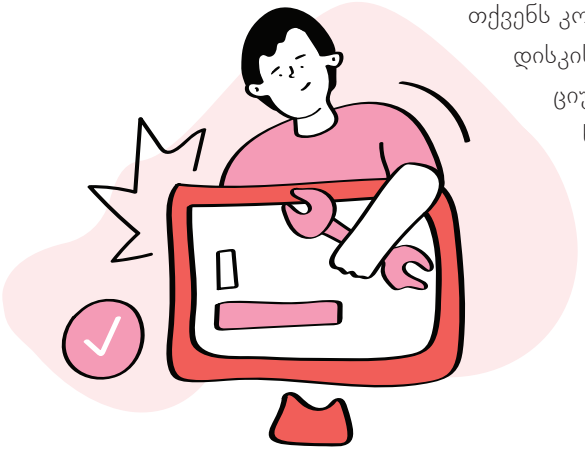
თქვენი მოწყობილობის დაშიფვრა

რაც შეეხება სმარტფონებს, Android და iOS მოწყობილობები დაშიფრულია ნაგულისხმევად. დაშიფვრამ რომ იმუშაოს, დარწმუნდით, რომ თქვენი სმარტფონი დაცულია ძლიერი პაროლით ან პასკოდით და რომ ის ავტომატურად დაბლოკავს ეკრანს ხანმოკლე უმოქმედობის შემდეგ. ასევე, დარწმუნდით, რომ თქვენს სმარტფონს აქვს ოპერაციული სისტემის უახლესი ვერსია.

კომპიუტერის დასაშიფრად უმარტივესი გზაა გამოიყენოთ უფასო, ჩაშენებული პროგრამული უზრუნველყოფა, რომელიც თან ახლავს ოპერაციულ სისტემას. Windows-საც და Mac-საც აქვთ ძლიერი ინსტრუმენტები დისკის სრული დაშიფვრისთვის. თუმცა, ეს ხელსაწყოები არ იმუშავებს, თუ არ დააკონფიგურებთ მათ თქვენს მოწყობილობაზე.

ასევე, დაფიქრდით გარე მყარი დისკებისა და მეხსიერების ბარათების დაშიფვრაზე. ასეთი მოწყობილობები ჩვეულებრივ აღჭურვილია ჩაშენებული დაშიფვრით.

როგორ დავშიფროთ Windows კომპიუტერები



თქვენს კომპიუტერზე პირადი მონაცემების დასაცავად, ყველაზე საიმედო გზა დისკის სრულად დაშიფვრაა. ამისთვის შეგიძლიათ გამოიყენოთ ოპერაციულ სისტემაში ჩაშენებული დასაშიფრი ხელსაწყოები. მაგრამ ეს ხელსაწყოები, დიდი ალბათობით, არ იმუშავებს თქვენს მოწყობილობაზე, სანამ მათ არ ჩართავთ.

გახსოვდეთ, დაშიფვრის რომელ ხელსაწყოსაც არ უნდა იყენებდეთ, თქვენი მონაცემები საიმედოდაა შენახული მხოლოდ იმ შემთხვევაში, თუ დაიცავთ თქვენს მოწყობილობას ძლიერი პაროლით და დააყენებთ ავტომატური დაბლოკვის რეჟიმს უმოქმედობის ხანმოკლე პერიოდის შემდეგ.

შეამოწმეთ, აქვს თუ არა თქვენს მოწყობილობას დაშიფვრის მხარდაჭერა

ზოგიერთ ძველ მოწყობილობას არ აქვს დაშიფვრის მხარდაჭერა, მაშინაც კი, თუ მასზე დაყენებულია Windows 10. იმის შესამოწმებლად, აქვს თუ არა თქვენს მოწყობილობას დაშიფვრის მხარდაჭერა, დააჭირეთ ღილაკს **დაწყება (Start)** გადადით **პარამეტრები** > **სისტემა** > **შესახებ** (**Settings > System > About**) და ნახეთ, პანელის ბოლოში აქვს თუ არა **მოწყობილობის დაშიფვრის (Device Encryption)** პარამეტრი.

თუ თქვენ გაქვთ **მოწყობილობის დაშიფვრის (Device Encryption)** პარამეტრი, შეგიძლიათ ჩართოთ ის Microsoft-ის ანგარიშით. თუ ის უკვე ჩართულია, კიდევ რაიმეს გაკეთება საჭირო აღარ არის.

თუ **მოწყობილობის დაშიფვრის** პარამეტრი არ ჩანს, ეს იმას ნიშნავს, რომ თქვენს მოწყობილობას არ აქვს დაშიფვრის მხარდაჭერა. თქვენ შეგიძლიათ გამოიყენოთ BitLocker-ის სტანდარტული დაშიფვრა, რომელიც ხელმისაწვდომია Windows 10-ის თითქმის ყველა ვერსიისთვის.

დაშიფვრის ჩართვა BitLocker-ით

BitLocker არის დაშიფვრის ხელსაწყო, რომელიც ჩაშენებულია Windows 10-ის Professional-ის, Enterprise-სა და Education-ის გამოცემებში. ის ხელმისაწვდომი არ არის Windows 10 Home-ის მქონე კომპიუტერებზე. თუ ზუსტად არ იცით Windows-ის რომელი ვერსია გაქვთ, შეგიძლიათ ნახოთ **პარამეტრები** > **სისტემა** > **შესახებ** (**Settings > System > About**) განყოფილებაში.

BitLocker-ით დაშიფვრის ჩასართავად, დარწმუნდით, რომ შესული ხართ თქვენს Windows მოწყობილობაში ადმინისტრატორის ანგარიშით. აირჩიეთ ღილაკი **დაწყება (Start)** და შემდეგ **Windows System-ის** ქვეშ, აირჩიეთ **Control Panel**. **Control Panel-ში**, აირჩიეთ **სისტემა და უსაფრთხოება (System and Security)** (თუ ვერ ხედავთ, დარწმუნდით, რომ "View by" დაყენებულია „Category"-ზე), გადადით **BitLocker Drive Encryption** > **Manage BitLocker**. აირჩიეთ **BitLocker-ის ჩართვა** და მიჰყევით ინსტრუქციებს.

BitLocker რომ დაყენდება, სულ პირველ დაშიფვრას შეიძლება დიდი დრო დასჭირდეს. ეს იმაზეა დამოკიდებული, რა მოცულობის ფაილები გაქვთ შენახული კომპიუტერში. თუმცა შეგიძლიათ, ჩვეულებრივად გამოიყენოთ კომპიუტერი, სანამ დისკის დაშიფვრა ხდება.

თუ თქვენ **System and Security-ის** პანელში არ გაქვთ პარამეტრი **BitLocker Drive Encryption**, შესაძლოა თქვენს მოწყობილობას არ ჰქონდეს **TPM** (Trusted Platform Module) ჩიპი, რომელსაც Windows დაშიფვრისთვის იყენებს. ამის შესამოწმებლად აირჩიეთ ღილაკი **დაწყება** და **Windows Administrative Tools-ის**

ქვეშ, აირჩიეთ **სისტემის ინფორმაცია (System Information)**. გადადით **სისტემის ინფორმაციის** ფანჯრის ბოლოში და იპოვეთ **მოწყობილობის დაშიფვრის მხარდაჭერა (Device Encryption Support)**.

თუ ღილაკის **მოწყობილობის დაშიფვრის მხარდაჭერის** გვერდით გიჩვენებთ, რომ („TPM გამოუყენებელია"), ეს ნიშნავს, რომ თქვენს მოწყობილობას არ აქვს TPM ჩიპი. BitLocker Encryption-ის ჩართვა შესაძლებელია ჩიპის გარეშეც. ამისათვის კლავიატურაზე დააჭირეთ **Windows Key + R ღილაკებს, გამოსულ ფანჯარაში ჩაწერეთ gpedit.msc და დააჭირეთ OK-ს. შემდეგ მიჰყევით მოცემულ ველებს** *Computer Configuration – Administrative Templates – Windows Components – BitLocker Drive Encryption – Operating System Drives.* ორჯერ სწრაფი დაჭერით გახსენით **Require additional authentication at startup. ნაგულისხმევად, ის დაყენებულია, როგორც Not Configured, ასე რომ თქვენ უნდა დააჭიროთ Enable რადიო ღილაკს. ამან ავტომატურად უნდა მონიშნოს Allow BitLocker without a compatible TPM ფუნქცია, თუ ეს არ მოხდა, დარწმუნდით, რომ ის მონიშნულია. ამის შემდეგ დააჭირეთ OK ღილაკს, დახურეთ ფანჯარა და დაუბრუნდით** BitLocker-ის ფანჯარას, რათა ჩართოთ ის.

თავი 5. ციფრული კომუნიკაცია

თავისუფალ და სამუშაო დროს სხვებთან კომუნიკაცია გვიწევს ელექტრონული ფოსტის, მესენჯერების, აუდიო და ვიდეო ზარების საშუალებით. ბოროტმოქმედები ცდილობენ, წვდომა მიიღონ ამ საუბრებზე და მოიპარონ თქვენი სენსიტიური ინფორმაცია. მოპარულ ინფორმაციას შემდგომ გამოიყენებენ თაღლითობისთვის, შანტაჟისთვის, დაშინებისთვის, ან თქვენი ვინაობის მოსაპარად. თქვენი საუბრების დასაცავად პირველი ნაბიჯია დაცული და დაშიფრული საკომუნიკაციო არხების გამოყენება.

დაიცავით თქვენი პირადი ციფრული საუბრები

ციფრული საუბრები ჩვენი ყოველდღიური პირადი და პროფესიული ცხოვრების მნიშვნელოვანი ნაწილი გახდა. ვურეკავთ მეგობრებსა და ოჯახის წევრებს WhatsApp-ის, ან Skype-ის საშუალებით, ვესაუბრებით მათ Facebook მესენჯერით და ვაგზავნით ელფოსტებს პირადი, სასწავლო, ან სამუშაო ანგარიშებიდან. გარდა ამისა, ვაგზავნით მოკლე ტექსტურ შეტყობინებებს ჩვენი მობილური ტელეფონებიდან და ვკამათობთ უცნობებთან ონლაინ ფორუმებზე.

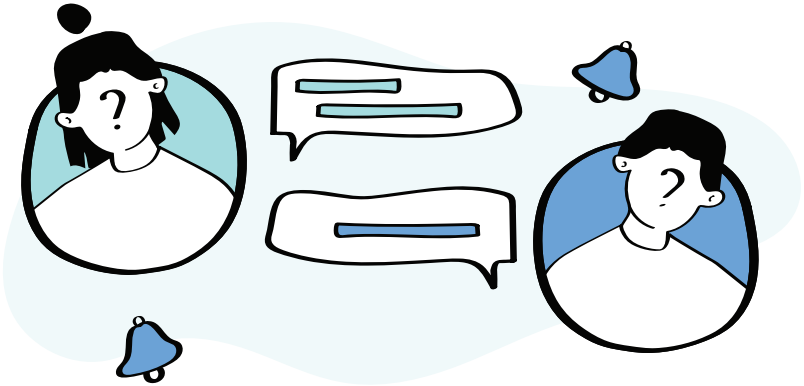
ყველა ეს საუბარი გადის რთულ ინფრასტრუქტურაში, მრავალი როუტერის, სერვერისა და კაბელის ჩათვლით. სხვადასხვა ადამიანს ან ორგანიზაციას, მოყვარული ჰაკერებისა და დახვეწილი ხელსაწყოებით აღჭურვილი ინტერნეტ პროვაიდერების ჩათვლით, შეუძლიათ, მიიღონ წვდომა ამ საუბრებზე. ციფრული კომუნიკაციის რომელ ტექნოლოგიასაც არ უნდა იყენებდეთ, აქ მოყვანილი ძირითადი რჩევები დაგეხმარებათ შეინარჩუნოთ თქვენი ონლაინ საუბრების კონფიდენციალურობა და უსაფრთხოება.

1. გამოიყენეთ ღია და დაშიფრული არხები

ბაზარზე ელფოსტისა და შეტყობინებების მრავალი სერვისია, მაგრამ თქვენი საუბრების კონფიდენციალურობასა და უსაფრთხოებას ყველა თანაბრად არ იცავს.

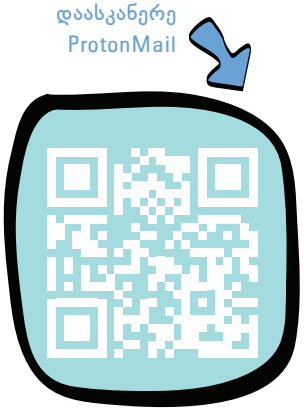
თუკი გსურთ, ვერავინ გაიგოს, რას უყვებით თქვენს თანამოსაუბრეს, გამოიყენეთ აპლიკაციები და სერვისები, რომლებიც გთავაზობენ ორმხრივ დაშიფვრას. როგორც ზემოთ აღვნიშნეთ, თქვენი ციფრული საუბრები გადის რთულ ინფრასტრუქტურაში და სანამ გაივლის, შეიძლება სხვადასხვა დაინტერესებული მხარის ხელში აღმოჩნდეს. თქვენი საუბრების დასაცავად არსებობს ერთადერთი საიმედო გზა: გამოიყენეთ სერვისები, რომლებიც შიფრავს (ანუ რთულ კოდად აქცევს) ყველაფერს, რაც ტოვებს თქვენს მოწყობილობას და არ გაშიფრავს მას მანამ, სანამ არ მივა ადრესატამდე. ვთქვათ, ვიღაცას „ხელში ჩა-

უვარდა“ დაშიფრული იმეილი ან ზარი თქვენს მოწყობილობასა და მიმღებს შორის. ამ შემთხვევაში, ის დაინახავს მხოლოდ უშინაარსო სიმბოლოების ერთობლიობას.



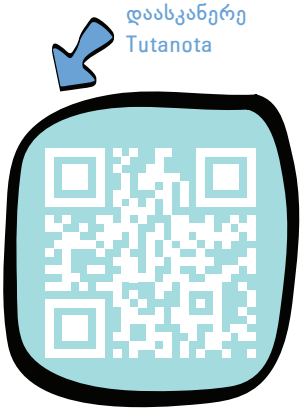
ასევე, უმჯობესია, აირჩიოთ ღია წყაროებზე დაფუძნებული აპლიკაციები და არა კერძო კომერციული პროდუქტები. პროგრამულ უზრუნველყოფას ეწოდება ღია წყაროზე დაფუძნებული, თუკი მისი კოდი ხელმისაწვდომია ყველასთვის, ვისაც მისი ნახვა სურს. ამ შემთხვევაში, დამოუკიდებელ ექსპერტებს და ტექნიკურად განსწავლულ მომხმარებლებს შეუძლიათ შეამოწმონ კოდი, რომლითაც აპლიკაციაა დაწერილი, აღმოაჩინონ და გამოასწორონ მასში არსებული სისუსტეები და დაადასტურონ, რომ აპლიკაცია საიმედოდ იცავს მომხმარებლის მონაცემებს.

დაასკანერე ProtonMail



ProtonMail და Tutanota გთავაზობთ უფასო, ღია წყაროზე დაფუძნებულ და ორმხრივად დაშიფრული ელფოსტის სერვისს, რომელიც იცავს თქვენს მიმოწერას. უფასო და ღია კოდზე დაფუძნებულ მესენჯერებს შორის, ორმხრივად დაშიფრული Wire და Signal საუკეთესო არჩევანია. თუ იყენებთ Telegram-ს, დარწმუნდით, რომ იყენებთ საიდუმლო ჩატებს (Telegram-ის სტანდარტული ჩატები დაშიფრული არ არის).

დაასკანერე Tutanota



2. დაიცავით თქვენი მოწყობილობები

სრული დაშიფვრა თქვენს საუბრებს უკანონო მიყურადებისგან იცავს, სანამ ისინი გზაშია თქვენსა და ადრესატს შორის. მაგრამ, ის ვერ დაგიცავთ, თუკი უკვე კონტროლდება თქვენი ან თქვენი თანამოსაუბრის მოწყობილობა. ეს შეიძლება მოხდეს, მაგალითად, თუკი უყურადღებოდ დატოვებთ თქვენს მოწყობილობას, ან დაკარგავთ მას ისე, რომ ეკრანის ავტომატური დაბლოკვა არ გექნებათ ჩართული. ეს ასევე შეიძლება მოხდეს, თუკი თქვენი მოწყობილობა დაინფიცირებულია მავნე პროგრამით. მავნე პროგრამა შესაძლოა თითქმის უხილავი იყოს, მაგრამ მას ბევრი რამე შეუძლია. მაგალითად, შეინახოს თქვენს მოწყობილობაზე აკრეფილი თითოეული ასო და გაუგზავნოს იგი სხვას.

ხშირად განაახლეთ თქვენი მოწყობილობების პროგრამული და აპარატული უზრუნველყოფა. ჩართეთ თქვენს მოწყობილობებზე ეკრანის ავტომატური დაბლოკვა ხანმოკლე უმოქმედობის შემდეგ. დარწმუნდით, რომ თქვენს დესკტოპებსა და ლეპტოპებზე დაყენებულია ანტივირუსული პროგრამა. გაიგეთ მეტი იმის შესახებ, თუ რა შეგიძლიათ გააკეთოთ თქვენი მოწყობილობების დასაცავად და თქვენი საუბრების უსაფრთხოების შესანარჩუნებლად.

3. შეწყვიტეთ მოკლე ტექსტური შეტყობინების გამოყენება

მოკლე ტექსტური შეტყობინებების სერვისი (SMS), რომელსაც იყენებენ ტელეფონზე ტექსტური შეტყობინებების მიმოცვლისთვის, მოძველებული და დაუცველია. პირველ რიგში იმიტომ, რომ მოკლე ტექსტური შეტყობინებები არ არის დაშიფრული. მათზე წვდომა შესაძლებელია განსაკუთრებით დახვეწილი ხელსაწყოების გარეშე. მეორე, ეს შეტყობინებები შეიცავს მეტამონაცემს, რომლითაც შეიძლება გამგზავნისა და მიმღების ვინაობის დადგენა. მესამე, მოკლე ტექსტური შეტყობინებების გაყალბება ადვილია, ანუ შესაძლებელია ისინი სხვის ნაცვლად გაიგზავნოს. ამდენად, დანამდვილებით ვერასოდეს გაიგებთ, კონკრეტული შეტყობინება სინამდვილეში ვისგან მიიღეთ. და ბოლოს, მობილური კავშირის პროვაიდერები ინახავენ მოკლე ტექსტურ შეტყობინებებსა და მათ მეტამონაცემებს დიდი ხნის განმავლობაში, ზოგჯერ სამუდამოდაც. ეს ზრდის იმის ალბათობას, რომ თქვენს საუბრებზე წვდომა ექნება სხვას, თან ისე, რომ ამას ვერც გაიგებთ.

თუკი გსურთ, რომ თქვენი შეტყობინებები სხვებმა ვერ ნახონ, გამოიყენეთ ორმხრივად დაშიფრული მესენჯერები, რომელიც ზემოთ ჩამოვთვალეთ. თუ სხვანაირად არ გამოდის, მოკლე ტექსტური შეტყობინებების ნაცვლად, გამოიყენეთ Android-ში, ან Apple-ში ჩაშენებული სამესიჯო სისტემები.

Apple მოწყობილობა

- Apple-ის მოწყობილობაზე, iMessage-ის ნაგულისხმევ სისტემად დასაყენებლად გადადით **პარამეტრებზე** > **შეტყობინებებზე (Settings > Notifications)** და ჩართეთ **iMessage**. ამ პარამეტრის ჩართვით, შეძლებთ სხვა ადამიანებს გაუგზავნოთ ტექსტური შეტყობინებები, ფოტოები, ვიდეო და აუდიო ფაილები iPhone-ის, iPad-ის ან Mac-ის გამოყენებით, დაშიფრული კავშირის საშუალებით.

ანდროიდ მოწყობილობა

- უახლესი Android მოწყობილობების უმეტესობას მოყვება Messages, Google-ის მონაცემთა ბაზაზე დაფუძნებული შეტყობინებების აპლიკაცია. თუ თქვენს Android მოწყობილობას არ აქვს Messages-ის აპი, ჩამოტვირთეთ ის Play Store-დან. Messages შეტყობინებების ნაგულისხმევი აპი რომ გახდეს, გადადით **პარამეტრებზე** > **აპებზე და შეტყობინებებზე** > **უპირატესზე** > **ნაგულისხმევ აპებზე** > **SMS აპლიკაცია (Settings > Apps and Notifications > Default Apps > SMS Application)** შემდეგ, აირჩიეთ Messages, როგორც თქვენი ნაგულისხმევი შეტყობინებების აპი.
- Messages აპის საშუალებით, დაშიფრული შეტყობინებების გასაგზავნად თქვენ უნდა ჩართოთ ჩატის ფუნქციები. ამისათვის თქვენს მოწყობილობაზე გახსენით Messages აპი და ზედა მარჯვენა კუთხეში შეეხეთ სამ ვერტიკალურ წერტილს. აირჩიეთ პარამეტრები > ჩატის ფუნქციები (Settings > Chat features) დააყენეთ **ჩატის ფუნქციების ჩართვა (Turn Chat Features On)**.
- თუ Messages აპი მიუწვდომელია თქვენს ქვეყანაში, ან თქვენი მოწყობილობებისთვის, გამოიყენეთ ის მესენჯერები, რომელიც ზემოთ ჩამოვთვალეთ.

4. წაშალეთ ძველი შეტყობინებები

თუ არ გინდათ, რომ თქვენს მოწყობილობაზე არსებული ტექსტური, ფოტო და ვიდეო შეტყობინებები ცნობისმოყვარეებმა ნახონ, შეგიძლიათ, პერიოდულად წაშალოთ ძველი შეტყობინებები. ასე უფრო მშვიდად იქნებით. სულ რომ დაკარგოთ მოწყობილობა, ან ვიღაცამ რომ წაგართვათ, სხვებს ვერ ექნებათ წვდომა თქვენს შეტყობინებებზე. ძველი შეტყობინებების წაშლა ასევე გამოანთავისუფლებს ადგილს თქვენს მოწყობილობაზე.

გირჩევთ, ჩართოთ თქვენს მოწყობილობაზე ძველი შეტყობინებების ავტომატური წაშლა. სამწუხაროდ, Android მოწყობილობებზე, Google Messages-ში ამას ვერ იზამთ. ამიტომ, Android მოწყობილობას თუ იყენებთ, ძველი შეტყობინებები ხელით უნდა წაშალოთ ხოლმე.

iPhone-სა თუ iPad-ზე ძველი შეტყობინებების ავტომატურად წაშლის დასაყენებლად გადადით **პარამეტრებზე** > **შეტყობინებები (Settings > Notifications)**. გადადით ქვემოთ **შეტყობინებების ისტორიაზე (Notifications History)** და დააწკაპუნეთ **შეტყობინებების შენახვაზე (Store Notification)**. აირჩიეთ **30 დღე,** რათა წაიშალოს ყველა შეტყობინება, რომელიც ერთ თვეზე ძველია. ამ პარამეტრის ჩართვის შემდეგ, თქვენი მოწყობილობა შეტყობინებას, მისი მოსვლიდან 30 დღეში, ავტომატურად წაშლის. თუ გსურთ, წაშალოთ შეტყობინებები, რომელიც უფრო ადრე მოგივიდათ, ამის გაკეთება ხელით მოგიწევთ.

გახსოვდეთ, თქვენს მოწყობილობაზე შეტყობინებები რომც წაშალოთ, ისინი არ წაიშლება მიმღების მოწყობილობაზე.

5. გამოიყენეთ გაუჩინარებადი (გარკვეულ დროზე გათვლილი) შეტყობინებები

მესენჯერების უმეტესობა საშუალებას გაძლევთ გააგზავნოთ შეტყობინებები, რომლებიც ქრება გარკვეული დროის, ან მას შემდეგ, რაც ადრესატი მათ ნახავს. ეს იცავს თქვენს შეტყობინებებს ცნობისმოყვარეებისგან, თუკი მოწყობილობას დაკარგავთ, ან მოგპარავენ (ან წაგართმევენ). ასე თქვენს შეტყობინებებს ვერც იმ ადამიანის მოწყობილობიდან ნახავენ, ვისაც ის გაუგზავნეთ.

ყველაფერი აწონ-დაწონეთ, ტექსტების, ფოტოების ან ვიდეოების გასაგზავნად, გაუჩინარებადი (გარკვეულ დროზე გათვლილი) შეტყობინებები გაცილებით უსაფრთხოა. გაითვალისწინეთ, ადრესატს თქვენი შეტყობინებების კოპირება და მოწყობილობაში შენახვა მაინც შეუძლია.

6. გამოიყენეთ ძლიერი პაროლები და ორეტაპიანი ავტორიზაცია

დაიცავით ყველა ელფოსტისა და მესენჯერის ანგარიში პაროლით, რომლის გამოცნობა ან გატეხვა შეუძლებელია. პაროლი ითვლება ძლიერად, თუ ის შეიცავს მინიმუმ 12 სიმბოლოს, მათ შორის დიდ და პატარა ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს. უძლიერეს პაროლებს ამ სიმბოლოების შემთხვევითი კომბინაციები ქმნის.

დარწმუნდით, რომ იყენებთ უნიკალურ პაროლს ყველა თქვენი ანგარიშისთვის. გაიგეთ მეტი იმაზე, თუ რატომ არის ცუდი ერთი და იგივე პაროლის გამოყენება სხვადასხვა ანგარიშებისთვის. ამდენი რთული და უნიკალური პაროლი ნუ დაგაფრთხობთ. შეგიძლიათ, გამოიყენოთ პაროლის მენეჯერი, რათა დაიმახსოვროთ და უსაფრთხოდ შეინახოთ ისინი.

სამწუხაროდ, ყველაზე ძლიერი პაროლიც კი შეიძლება მოიპაროონ სხვადასხვა გზით. სწორედ ამიტომ უნდა გამოიყენოთ ორეტაპიანი ავტორიზაცია (2FA) თქვენი ელ ფოსტისა და მესენჯერის ანგარიშების დასაცავად. ორეტაპიანი ავტორიზაციის ჩართვის შემდეგ, თქვენი ვინაობის დასადასტურებლად მეორე გზაც უნდა გამოიყენოთ.

ორეტაპიანი ავტორიზაციის ყველაზე უსაფრთხო გზაა, დააყენოთ თქვენს ტელეფონზე აპლიკაცია, რომელიც გამოიმუშავებს დროებით ციფრულ კოდებს. სოციალურ ქსელში თქვენი ანგარიშის პაროლს რომ შეიყვანთ, მერე კოდის შეყვანაც დაგჭირდებათ (იხ. თავი 1).

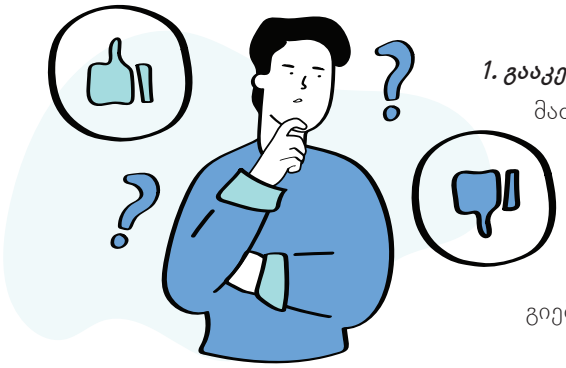
7. დაფიქრდით, სანამ გააგზავნით

ეს მართლაც მარტივია: ტექსტური, ფოტო ან ვიდეო შეტყობინების გაგზავნამდე იმაზე დაფიქრდით, ამას ოდესმე თუ ინანებთ. გაგზავნის ღილაკზე დაჭერის შემდეგ, ვეღარ გააკონტროლებთ, თუ ვის ექნება თქვენი შეტყობინების ასლი. თუ რამე ძალიან პირადის, კონფიდენციალურის ან სენსიტიურის გაზიარება გსურთ, პირისპირ შეხვედრა საუკეთესო გამოსავალია.

როგორ ავირჩიოთ უსაფრთხო საკომუნიკაციო პლატფორმა

როდესაც მობილური მოწყობილობიდან შეტყობინებას აგზავნით, ჩვეულებრივ, არ ფიქრობთ იმ აპლიკაციების უსაფრთხოების შეზღუდვებზე, რომლებსაც იყენებთ. თქვენ, შესაძლოა, არ უღრმავდებით, თუ რამდენად დაუცველია თქვენი მონაცემები და თუ სენსიტიურ პერსონალურ ინფორმაციას შეტყობინებაში გააზიარებთ, ის შეიძლება არასწორი ადამიანის ხელში აღმოჩნდეს.

გაზრდილი დაცვისთვის, ზოგიერთი მომხმარებელი ირჩევს დაშიფრული შეტყობინებების აპლიკაციის გამოყენებას. მაგრამ, ყველა დაშიფრული შეტყობინებების აპლიკაცია არ არის შექმნილი თანაბარი შესაძლებლობებითა და დაცვით. თქვენთვის შესაფერისი აპლიკაციის ასარჩევად, მიჰყევით ამ 6 რჩევას.



1. გააკეთეთ თქვენი კვლევა

მათთვის, ვინც კომუნიკაციის უსაფრთხოებაზე ზრუნავს, ორმხრივი დაშიფვრის მქონე შეტყობინების კარგი აპლიკაციების პოვნა ადვილი უნდა იყოს. ზოგიერთმა ასეთმა აპლიკაციამ უკვე გაიარა დროის გამოცდა და მათი რეპუტაცია საკმაოდ მყარია. მსგავსი აპლიკაციის არჩევის დროს ყურადღება უნდა მიაქციოთ გამოყენებულ ტექნოლოგიებს, მომსახურების მიმწოდებლის პოლიტიკასა და მის გამოცდილებას.

2. ფრთხილად იყავით რას წერთ

მიუხედავად იმისა, რომ ბევრი აპლიკაცია მოწოდებულია თქვენთვის, როგორც უსაფრთხო და დაშიფრული, თითქმის ყველა შემთხვევაში, ელექტრონული ან წერილობითი კომუნიკაციის ამოღება იურიდიულად შესაძლებელი და დაუცველია. ნებისმიერი კომუნიკაციის გატეხვა შესაძლებელია, რომელსაც ინტერნეტთან აქვს წვდომა. თუ თქვენ მნიშვნელოვანი და სენსიტიური ინფორმაცია გაქვთ გადასაცემი მეორე მხარისთვის, გამოიყენეთ სხვა (ოფლაინ) ხერხები.

3. დააინსტალირეთ მხოლოდ ის აპლიკაციები, რომლებსაც იყენებთ

ვინაიდან ბევრი ადამიანი დეტალებს ყურადღებას არ აქცევს, იყავით ფრთხილად და დააინსტალირეთ მხოლოდ ის პალიკაციები, რომლებიც გჭირდებათ და იყენებთ. Google-ის მომხმარებლებმა, შეამოწმეთ თქვენი უსაფრთხოების პარამეტრები და წაშალეთ აპლიკაციები, რომლებსაც აღარ იყენებთ, მაგრამ აქვთ წვდომა თქვენს მონაცემებზე. შეიძლება გაგიკვირდეთ, რამდენ აპლიკაციას აქვს წვდომა თქვენს ინფორმაციაზე.

4. გამოიყენეთ ღია კოდზე დაფუძნებული პროგრამული უზრუნველყოფა, რომელმაც დამოუკიდებლად გაიარა შემოწმება

მაქსიმალური უსაფრთხოებისთვის აირჩიეთ აპლიკაცია, რომელიც არის ღია კოდით შექმნილი, დამოუკიდებელი ექსპერტების მიერ შემოწმებული და არ ინახავს თქვენს მეტამონაცემებს, როგორიცაა, მაგალითად, Signal. შემდეგ აარჩიეთ ისეთი აპლიკაცია, რომლის დაცვაც შესაძლებელია პინ-კოდით (როგორც ორეტაპიანი ავტორიზაცია) და გააჩნია გაუჩინარებადი შეტყობინებების ფუნქცია. და ბოლოს, გესმოდეთ, რომ ნებისმიერი აპლიკაციის ან ტელეფონის გატეხვა შესაძლებელია, ასე რომ, შესაბამისად გაფილტრეთ თქვენ მიერ გაგზავნილი შეტყობინების შენაარსის მგრძნობელობა.

5. გაიგეთ მეტი სხვების გამოცდილების შესახებ

თქვენი კომუნიკაციის დასაცავად, ძალიან მნიშვნელოვანია ორმხრივი დაშიფვრა და კარგია თუ ამ ფუნქციის მქონე აპლიკაციას იყენებთ. მაგრამ გაითვალისწინეთ, რომ როდესაც ხალხი აღფრთოვანებულია ბაზარზე ახალი აპლიკაციის გამოჩენით, თქვენთვის მთავარია იმის გააზრება, რომ ყველა მომხმარებელი ერთნაირი არ არის. ამიტომ, დაფიქრდით, გჭირდებათ თუ არა ამ აპლიკაციის დაყენება თქვენს მოწყობილობაზე. სტუდენტი, რომელიც ესაუბრება მეგობრებს, ძალიან განსხვავებული შემთხვევაა, ვიდრე საჯარო მოხელე, რომელიც იყენებს ამა თუ იმ ჩატის აპლიკაციას. თქვენ, როგორც საჯარო მოხელეს, სხვა პასუხისმგებლობა გაკისრიათ მონაცემთა დასაცავად.

6. აირჩიეთ აპლიკაცია იდენტობის დადასტურების ვრცელი პროცესებით

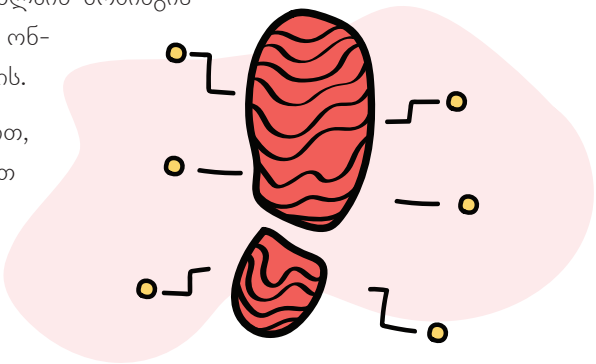
მომხმარებლებმა, განსაკუთრებით საჯარო მოხელეებმა, უნდა აირჩიონ აპლიკაცია ვრცელი, ინდეტობის გადამოწმების პროცესით, რათა უზრუნველყონ უსაფრთხო კომუნიკაცია როგორც სამუშაო, ასევე პირადი შეტყობინებებისთვის. ასევე, გაითვალისწინეთ, რომ დაშიფრული შეტყობინებები ტელეფონში რჩება, თუ მათ არ წავშლით, ამიტომ, გირჩევთ დააყენოთ შეტყობინებების ვადა ისე, რომ გარკვეული დროის გასვლის მერე, ისინი ავტომატურად წაიშალოს.

თავი 6. ციფრული იდენტობა

ციფრული იდენტობა ის ინფორმაციაა, რომელიც ონლაინ არსებობს ცალკეული ადამიანებისა და ორგანიზაციების შესახებ. ყოველ ჯერზე, როდესაც ინტერნეტში შედიხართ, სულ ერთია, რომელი მოწყობილობიდან, თქვენ დიდი რაოდენობით მონაცემებს ტოვებთ. ეს ინფორმაცია შეიძლება გამოიყენონ თქვენთვის რეკლამების უკეთ „დასამიზნებლად“, თქვენზე სათვალთვალოდ, ან სოციალური ინჟინერიით თქვენთვის თავგზის ასაბნევად.

რა კვალს ვტოვებთ ინტერნეტში შესვლისას

ციფრული კვალი, რომელსაც ზოგჯერ ციფრულ ჩრდილს ან ელექტრონულ კვალს უწოდებენ, ეხება იმ მონაცემების კვალს, რომელსაც ტოვებთ ინტერნეტის გამოყენებისას. ციფრული კვალი შეიძლება დატოვოთ ვებსაიტებზე შესვლით, მეილის გაგზავნით, სოციალურ მედიაში პოსტის დადებით, საინფორმაციო ბიულეტენის გამოწერით, ონლაინ მიმოხილვის დატოვებით ან ონლაინ შოპინგის დროს. ეს ყველაფერი კი, შეიძლება გამოყენებულ იქნას ადამიანის ონლაინ აქტივობებისა და მოწყობილობების თვალყურის დევნებისთვის.



თუმცა, ჩვეულებრივი მომხმარებლები, ყოველთვის ვერ ვხვდებით, როდის ვტოვებთ ამ კვალს. მაგალითად, ვებსაიტებს შეუძლიათ თვალყური ადევნონ თქვენს აქტივობას თქვენს მოწყობილობაზე ქუქი-ფაილების (cookies) დაყენებით, ხოლო აპლიკაციებს შეუძლიათ თქვენი მონაცემების შეჯერება ისე, რომ თქვენ ამის შესახებ წარმოდგენა არ გქონდეთ. მას შემდეგ, რაც რომელიმე ვებგვერდს ან აპლიკაციას თქვენს ინფორმაციაზე წვდომის უფლებას მისცემთ, მათ შეუძლიათ გაყიდონ ან გაუზიარონ თქვენი მონაცემები მესამე მხარეებს. კიდევ უარესი, თქვენი პერსონალური ინფორმაცია შეიძლება იყოს კომპრომეტირებული და ის საჯაროდ ხელმისაწვდომი გახდეს.

რატომ აქვს მნიშვნელობა ციფრულ კვალს

ციფრული კვალი მნიშვნელოვანია, რადგან:

- ისინი შედარებით მუდმივია და როგორც კი მონაცემები საჯაროა, ან თუნდაც ნახევრად საჯარო, როგორც ეს შეიძლება იყოს Facebook პოსტების შემთხვევაში, მფლობელს მცირე კონტროლი აქვს იმაზე, თუ როგორ გამოიყენებენ მას სხვები.
- ციფრულ კვალს შეუძლია განსაზღვროს ადამიანის ციფრული რეპუტაცია, რომელიც დღესდღეობით ისეთივე მნიშვნელოვანია, როგორც მათი ოფლაინ რეპუტაცია, ეს განსაკუთრებით მნიშვნელოვანია საჯარო მოხელეებისთვის.

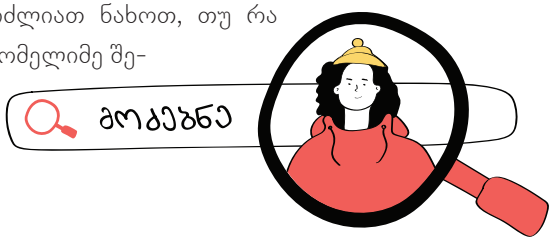
- დამსაქმებლებს შეუძლიათ შეამოწმონ თავიანთი პოტენციური თანამშრომლების ციფრული კვალი, განსაკუთრებით მათი სოციალური მედია, დასაქმების გადაწყვეტილების მიღებამდე.
- სიტყვები და ფოტოები, რომლებსაც ინტერნეტში აქვეყნებთ, შეიძლება არასწორად იქნას განმარტებული ან შეცვლილი, რამაც შესაძლოა გამოიწვიოს უნებლიე შეურაცხყოფა ვინმეს მისამართით.
- ინფორმაცია, რომელიც განკუთვნილია კერძო ჯგუფისთვის, შეიძლება გავრცელდეს უფრო ფართო წრეში, რამაც შეიძლება ზიანი მიაყენოს ურთიერთობებსა და მეგობრობას.
- კიბერკრიმინალებს შეუძლიათ გამოიყენონ თქვენი ციფრული კვალი ისეთი მიზნებისთვის, როგორიცაა ფიშინგი ანგარიშზე წვდომისთვის ან ყალბი პირადობის შექმნა თქვენს მონაცემებზე დაყრდნობით.

დაიცავით თქვენი ციფრული კვალი

იმის გამო, რომ დამსაქმებლებს და სხვა დაინტერესებულ პირებს შეუძლიათ მოიძიონ თქვენი ონლაინ იდენტობა, ყურადღება მიაქციეთ თქვენს ციფრულ კვალს. აქ მოცემულია რამდენიმე რჩევა თქვენი პერსონალური მონაცემების დასაცავად და თქვენი ონლაინ რეპუტაციის სამართავად.

გამოიყენეთ საძიებო სისტემები თქვენი ციფრული ანაბეჭდის შესამოწმებლად

შეიყვანეთ თქვენი სახელი საძიებო სისტემებში, სადაც შეგიძლიათ ნახოთ, თუ რა ინფორმაციაა თქვენს შესახებ საჯაროდ ხელმისაწვდომი. თუ რომელიმე შედეგი უარყოფითად გახასიათებთ, შეგიძლიათ დაუკავშირდეთ საიტის ადმინისტრატორს, რათა ნახოთ, შეუძლიათ თუ არა მისი წაშლა. ასევე, შეგიძლით გამოიყენოთ Google Alerts-ის



ფუნქცია, რომელიც თქვენი სახელის გამოყენების შემთხვევაში შეტყობინებას გამოგიგზავნით.

დაასკანერე whitepages.com

შეამცირეთ ინფორმაციის წყაროების რაოდენობა, სადაც ნახსენები ხართ

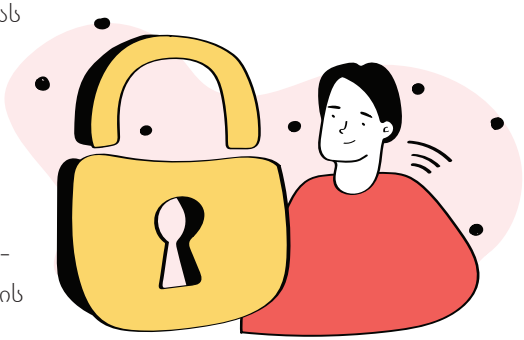
მაგალითად, უძრავი ქონების ვებსაიტებსა და whitepages.com-ს შეიძლება ჰქონდეს მეტი ინფორმაცია თქვენს შესახებ, ვიდრე თქვენ გსურთ. ეს საიტები ხშირად შეიძლება შეიცავდეს პერსონალურ ინფორმაციას, როგორიცაა თქვენი ტელეფონის ნომერი, მისამართი და ასაკი. თუ ეს არ გსიამოვნებთ, შეგიძლიათ დაუკავშირდეთ ვებგვერდებს და მოითხოვოთ ინფორმაციის წაშლა.

შეზღუდეთ თქვენ მიერ გაზიარებული მონაცემების რაოდენობა

ყოველ ჯერზე, როცა სხვას უგზავნით თქვენს პირად ინფორმაციას, ამით აფართოებთ თქვენს ციფრულ კვალს. იმ შემთხვევაში თუ მიმღები დაკარგავს თქვენ მიერ გაგზავნილ მონაცემებს, ისინი შეიძლება ცუდ ხელში მოხვდნენ. ასე რომ, კარგად დაფიქრდით, ვის უგზავნით თქვენს მონაცემებს და რამდენად სანდოა მიმღები.

შეამოწმეთ თქვენი კონფიდენციალურობის პარამეტრები სოციალურ მედიაში

კონფიდენციალურობის პარამეტრები სოციალურ მედიაში საშუალებას გაძლევთ, აკონტროლოთ ვინ ხედავს თქვენს პოსტებს და ინფორმაციას თქვენზე. გადახედეთ ამ პარამეტრებს და დარწმუნდით, რომ ისინი დაყენებულია თქვენთვის კომფორტულ დონეზე. მაგალითად, Facebook საშუალებას გაძლევთ შეზღუდოთ შეტყობინებები მხოლოდ მეგობრებით და შექმნათ იმ ადამიანების სიები, რომლებსაც შეუძლიათ გარკვეული პოსტების ნახვა. თუმცა, გაითვალისწინეთ, რომ კონფიდენციალურობის პარამეტრები გიცავთ მხოლოდ შესაბამისი სოციალური მედიის საიტზე.



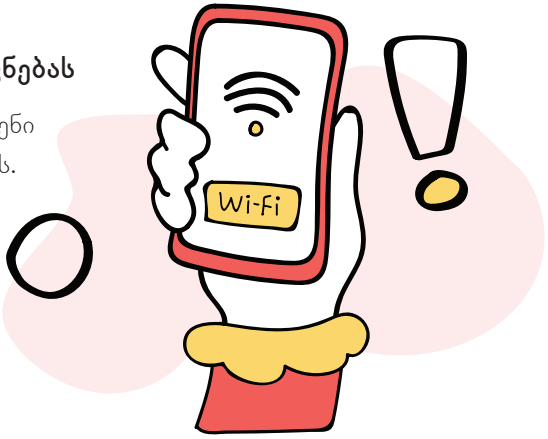
მოერიდეთ გადაჭარბებულ გაზიარებას სოციალურ მედიაში

სოციალური მედია აადვილებს სხვებთან დაკავშირებას, მაგრამ ასევე შეუძლია გააადვილოს ზედმეტი გაზიარება. ორჯერ დაფიქრდით, სანამ გამოაქვეყნებთ თქვენს მდებარეობას, მოგზაურობის გეგმებს ან სხვა პირად ინფორმაციას. მოერიდეთ თქვენი ტელეფონის ნომრის ან ელფოსტის მისამართის თქვენს სოციალური მედიის ბიოში გამჟღავნებას. ასევე კარგი იდეაა, მოერიდოთ თქვენი ბანკის, ჯანდაცვის პროვაიდერის, საყვარელი აფთიაქის და ა.შ. „მოწონებას“ – რადგან ამან შეიძლება კიბერკრიმინალები თქვენს კრიტიკულ ანგარიშებამდე მიიყვანოს.

მოერიდეთ სახიფათო ვებსაიტებს

როდესაც ონლაინ რამეს ყიდულობთ და საბანკო ბარათის გამოყენება გიწევთ, დარწმუნდით, რომ ტრანზაქციას უსაფრთხო ვებსაიტზე აწარმოებთ – გვერდის მისამართი უნდა დაიწყოს https://-ით და არა http://-თი – „s“ ნიშნავს „უსაფრთხოს“ და მიუთითებს, რომ საიტს აქვს უსაფრთხოების სერტიფიკატი. ასევე, უნდა იყოს ბოქლომის ხატულა მისამართების ზოლის მარცხნივ. არასოდეს გააზიაროთ რაიმე კონფიდენციალური ინფორმაცია დაუცველ საიტებზე, განსაკუთრებით პერსონალური ინფორმაცია და საბანკო ბარათის მონაცემები.

მოერიდეთ საჯარო Wi-Fi-ზე პირადი მონაცემების გამჟღავნებას



საჯარო Wi-Fi ქსელი არსებითად ნაკლებად დაცულია, ვიდრე თქვენი პირადი, რადგან არ იცით ვინ დააყენა ან ვინ შეიძლება მის უკან იდგეს. მოერიდეთ პირადი ინფორმაციის გაგზავნას საჯარო Wi-Fi ქსელების გამოყენებისას.

წაშალეთ ძველი ანგარიშები

თქვენი ციფრული ანაბეჭდის შემცირების ერთ-ერთი გზაა ძველი ანგარიშების წაშლა. მაგალითად, სოციალური მედიის პროფილები, რომლებსაც აღარ იყენებთ ან საინფორმაციო გამოწერები, რომლებსაც აღარ კითხულობთ. „მიძინებული“ ანგარიშებისგან თავის დაღწევა ამცირებს თქვენზე არსებული მონაცემების გავრცელებას.

არ შეხვიდეთ Facebook-ით სხვა ანგარიშებზე

ვებსაიტებსა და აპლიკაციებში Facebook-ის გამოყენებით შესვლა მოსახერხებელია. თუმცა, ყოველ ჯერზე, როდესაც სხვა ვებგვერდზე Facebook-ით შედიხართ, თქვენ ამ გვერდს აძლევთ უფლებას გამოიყენოს თქვენი მომხმარებლის მონაცემები, რაც ცხადია, თქვენს პერსონალურ ინფორმაციას რისკის ქვეშ აყენებს.

დაფიქრდით, სანამ გამოაქვეყნებთ

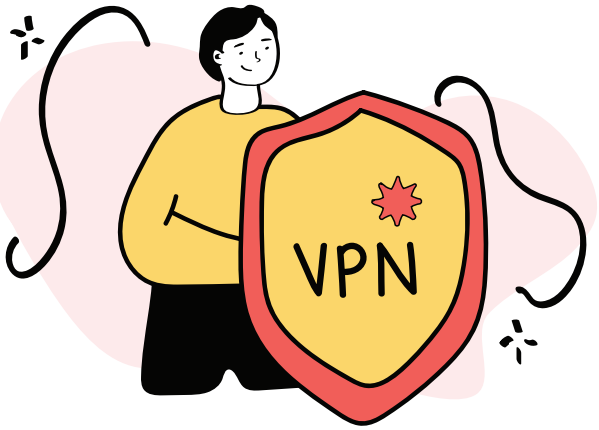
ის, რასაც თქვენ აქვეყნებთ ან ამბობთ ონლაინ, ქმნის თქვენზე წარმოდგენას. თქვენი ციფრული ანაბეჭდის ასპექტები, როგორიცაა ატვირთული ფოტოები, ბლოგის კომენტარები, YouTube ვიდეოები და Facebook პოსტები, შესაძლოა არ ასახავდეს ინფორმაციას ისე, როგორც თქვენ ისურვებდით. ამიტომ, სანამ გამოაქვეყნებთ, კარგად დაფიქრდით, რა სახის ინფორმაციაა ის.

ინფორმაციის გაჟონვის შემთხვევაში, იმოქმედეთ სწრაფად

თუ გაუთვალისწინებელი შემთხვევა მოხდა, ან ეჭვი შეგეპარათ, რომ თქვენმა პერსონალურმა ინფორმაციამ გაჟონა ან ვინმემ მოიპარა, დაუყოვნებლივ მიიღეთ ზომები. თუ დარღვევა ფინანსურ ზარალთან არის დაკავშირებული, დაუკავშირდით თქვენს ბანკს ან საკრედიტო ბარათის პროვაიდერს. შეცვალეთ ნებისმიერი პაროლი, რომელიც შესაძლოა გამჟღავნებულიყო. თუ იგივე პაროლს სხვა ანგარიშებისთვისაც იყენებ, დაუყოვნებლივ შეცვალეთ პაროლი ყველგან.

გამოიყენეთ VPN

ვირტუალური კერძო ქსელის ან VPN-ის გამოყენება დაგეხმარებათ თქვენი ციფრული ანაბეჭდის დაცვაში. ეს იმიტომ ხდება, რომ VPN ნიღბავს თქვენს IP მისამართს, რაც თქვენს ონლაინ მოქმედებებს პრაქტიკულად მიუწვდომელს ხდის. ეს იცავს თქვენს კონფიდენციალურობას ონლაინ და შეუძლია ხელი შეუშალოს ვებსაიტებს „ქუქის„-ების დაყენებაში, რომლებიც თვალყურს ადევნებენ თქვენს ინტერნეტ დათვალიერების ისტორიას.



როგორ დავიცვათ პერსონალური ინფორმაცია სოციალურ ქსელებში

თუ სხვების მსგავსად, თქვენც დიდ დროს ატარებთ სოციალურ ქსელებში, მაშინ დიდი შანსია, ბევრ პირად ინფორმაციას აზიარებდეთ. სოციალური ქსელების მეშვეობით თქვენზე ბევრი რამე შეიძლება გაიგონ, მაგალითად: თქვენი სრული სახელი, სკოლა, სამსახური, ოჯახის წევრების და მეგობრების ვინაობა, საცხოვრებელი, ან ადგილი, რომელსაც ხშირად სტუმრობთ, ჰობი და ინტერესები, პოლიტიკური შეხედულებები, მუსიკალური გემოვნება და ასე შემდეგ.

ეს ინფორმაცია შეიძლება გამოიყენონ თქვენ წინააღმდეგ. თაღლითებს შეუძლიათ გამოიყენონ თქვენი პერსონალური მონაცემები, თავი მოაჩვენონ თქვენს მეგობრებს ან კოლეგებს, თითქოს ეს თქვენ ხართ და გამოსტყუონ ფული, ან სენსიტიური ინფორმაცია. მათ ასევე შეუძლიათ გამოიყენონ ის ინფორმაცია, რომელსაც აქვეყნებთ, რათა გამოიცნონ თქვენი უსაფრთხოების კითხვები საბანკო ან გაცნობისათვის განკუთვნილ საიტებზე, მოიპარონ თქვენი ონლაინ ანგარიშები, ან შეგაწუხონ.

კარგი ამბავი ისაა, რომ ქვემოთ ჩამოთვლილი რამდენიმე სწრაფი და მარტივი ხერხი დაგეხმარებათ თქვენი პერსონალური ინფორმაციის უსაფრთხოდ შენახვაში, თან ისე, რომ სოციალური ქსელები მაინც უპრობლემოდ გამოიყენოთ.

1. გამოიყენეთ ძლიერი და უნიკალური პაროლები

დაიცავით სოციალური მედიის ყველა ანგარიში პაროლით, რომლის გამოცნობა ან გატეხვა შეუძლებელია. პაროლი ძლიერია, როდესაც ის შედგება მინიმუმ 12 სიმბოლოსაგან, მათ შორის „დიდი“ და „პატარა“ ასოებისგან, რიცხვებისგან და სპეციალური სიმბოლოებისგან. ამ სიმბოლოების შემთხვევითი კომბინაციები ქმნის ყველაზე ძლიერ პაროლს. წაიკითხეთ უფრო მეტი იმის შესახებ, თუ როგორ შექმნით პაროლები, რომელთა გატეხვაც ძალიან რთულია.

2. დაამატეთ დაცვის მეორე დონე

სამწუხაროდ, ყველაზე ძლიერი პაროლიც კი შეიძლება მოიპარონ ან სხვაგვარად გატეხონ. სწორედ ამიტომ უნდა გამოიყენოთ ორნაბიჯიანი ავტორიზაცია (2FA) თქვენი სოციალური მედიის ანგარიშების დასა-

ცავად. როდესაც ჩართულია 2FA, პაროლის შეყვანის გარდა, დამატებით გთხოვენ, გამოიყენოთ თქვენი ვინაობის დამადასტურებელი მეორე გზაც.

2FA-ს გამოყენებისას, ყველაზე უსაფრთხო გზაა, დააყენოთ თქვენს ტელეფონზე აპლიკაცია, რომელიც დააგენერირებს დროებით ციფრულ კოდებს. სოციალური მედიის ანგარიშში შესასვლელად, პაროლის შეყვანისთანავე, ამ კოდის შეყვანაც მოგიწევთ.

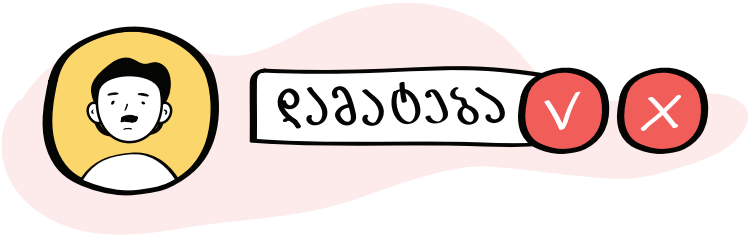
3. თქვენი პროგრამული უზრუნველყოფა ყოველთვის განახლებული უნდა იყოს

კიბერკრიმინალები სულ უფრო კარგად იყენებენ სხვადასხვა აპლიკაციებში ნაპოვნ დაუცველობებს მოწყობილობებში შესაღწევად. ამიტომ, ძალიან მნიშვნელოვანია თქვენი პროგრამული უზრუნველყოფა მუდმივად განახლებული იყოს. დარწმუნდით, რომ მოწყობილობაზე, რომელსაც იყენებთ სოციალური მედიის ანგარიშებზე წვდომისთვის, ყოველთვის დაყენებულია ოპერაციული სისტემის უახლესი ვერსია. კომპიუტერს იყენებთ თუ მობილურს, დარწმუნდით, რომ ჩართულია ანტივირუსი და მასზე დაყენებულია ავტომატური განახლების რეჟიმი.

თუ შედიხართ სოციალურ მედია საიტებზე ვებბრაუზერის მეშვეობით, დარწმუნდით, რომ ისიც განახლებულია უახლეს ვერსიამდე. თუ მობილურ მოწყობილობაზე იყენებთ სოციალური მედიის ცალკეულ აპლიკაციებს, მაშინ ხშირად განაახლეთ ისინი.

4. იცოდეთ, ვის ამატებთ მეგობრებში

ეს საკმაოდ მარტივია: რაც უფრო მეტ ადამიანთან ხართ დაკავშირებული, მით უფრო რთულია იმის კონტროლი, თუ რა მოუვა პერსონალურ ინფორმაციას, რომელსაც აზიარებთ სოციალურ ქსელში. თუ ძალიან მნიშვნელოვანი არაა, რომ თქვენი სოციალური მედიის ანგარიშები ყველასთვის იყოს ღია, დაფიქრდით, თუ ვის შეუზღუდავდით წვდომას თქვენს პოსტებსა და ფოტოებზე.



კარგი იქნება, თუ პერიოდულად გადახედავთ ხოლმე თქვენს მიმდევრებს სხვადასხვა სოციალურ ქსელში. დაფიქრდით იმ ადამიანების წაშლაზე, ვისაც აღარ ენდობით ან ვისთანაც აღარ გაქვთ კომუნიკაცია. თუ მომხმარებელი ითხოვს თქვენს პერსონალურ ინფორმაციას, გაწუხებთ, ან საეჭვოდ იქცევა, დაფიქრდით მისი პროფილის დაბლოკვაზე და დაარეპორტეთ იგი.

5. მართეთ თქვენი კონფიდენციალურობის პარამეტრები

სოციალური ქსელები შექმნილია იმისთვის, რომ თქვენი პოსტები და ფოტოები ხელმისაწვდომი გახდეს რაც შეიძლება მეტი მომხმარებლისთვის მთელი მსოფლიოს მასშტაბით. საბედნიეროდ, ეს სერვისები ასევე გეხმარებათ, მართოთ კონფიდენციალურობის ნაგულისხმევი პარამეტრები, რათა ზუსტად გააკონტროლოთ, თუ რა ინფორმაციის ნახვა შეუძლიათ სხვებს. მაგალითად, სოციალური მედიის საიტების უმეტესობა საშუალებას გაძლევთ შეზღუდოთ ვის შეუძლია თქვენი პროფილის ნახვა, დაბლოკოთ კონკრეტული მომხმარებლების პროფილები, გაუზიაროთ ფოტოები მხოლოდ კონკრეტულ ადამიანებს და ა. შ. დარწმუნდით, რომ უკვე გაერკვიეთ ამ პარამეტრების გამოყენებაში და თქვენი კონფიდენციალურობის დაცვაში.

6. შეინახეთ პირადი ინფორმაცია სოციალური მედიის მიღმა

სოციალური ქსელები გაძლევთ შესაძლებლობას, დაამატოთ უამრავი პირადი დეტალი, რათა დაეხმაროთ სხვებს თქვენს პოვნაში. რომელ სკოლაში დადიოდით? დაოჯახებული ხართ თუ არა? თქვენი ოჯახიდან ჩვენი ანგარიში კიდევ ვის აქვს? ამ დეტალების წყალობით სოციალურ ქსელში თქვენი ძალიან პირადი პორტრეტი იხატება. იგი ნამდვილი საგანძურია არაკეთილსინდისიერი ადამიანებისთვის.

შეეცადეთ აკონტროლოთ, თუ რა პირად ინფორმაციას აქვეყნებთ. მიაქციეთ ყურადღება თქვენი ბიოგრაფიის დეტალებს, ოჯახურ კავშირებსა და ფოტოებს. არასოდეს გააზიაროთ თქვენი პირადობის მოწმობის, კონცერტის, ან ავიაბილეთების ფოტოები. წინასწარ დაფიქრდით ხოლმე და გახსოვდეთ, რაიმეს თუ გამოაქვეყნებთ, თითქმის შეუძლებელია ზუსტად იმის გარკვევა, თუ ვის ექნება წვდომა ამ ინფორმაციაზე.

7. არ გააზიაროთ თქვენი ადგილმდებარეობა

ბოროტმოქმედებს ხშირად ისიც უადვილებს საქმეს, რომ ზოგი ყველას უზიარებს თუ სად იმყოფება და სად დადის ყველაზე ხშირად. ამას ვაკეთებთ, როდესაც სადმე „ვჩექინდებით„, ვაქვეყნებთ ფოტოებს, რომლებზეც ჩანს სად ვიმყოფებით, ან როდესაც ვყვებით დრო სად და როგორ გავატარეთ.

თუ ზრუნავთ საკუთარ კონფიდენციალურობაზე და პირად უსაფრთხოებაზე, მაშინ კარგი იქნება, თუ არ გაუზიარებთ თქვენს მდებარეობას სხვებს. გამორთეთ თქვენს მოწყობილობებზე მდებარეობის გაზიარების ფუნქცია და დაარეგულირეთ კონფიდენციალურობის პარამეტრები სოციალურ ქსელებში, რათა მათ შეწყვიტონ თქვენი ადგილმდებარეობის კონტროლი. არ გამოიყენოთ „დაჩექინების“ ფუნქციები და არ გამოაქვეყნოთ ფოტოები, სადაც ჩანს, სად იმყოფებით. ყოველ შემთხვევაში იქამდე მაინც, სანამ არ დატოვებთ იმ ადგილს.

8. არ გამოიყენოთ თქვენი სოციალური პროფილები სხვა ვებსაიტებზე შესასვლელად

ახალი ონლაინ ანგარიშის შექმნისას შესაძლოა, გაგიჩნდეთ ცდუნება და გამოიყენოთ ფუნქცია „შესვლა Facebook-ის მეშვეობით„. ასეთ დროს თქვენ ენდობით გარე საიტს, რომელშიც შედიხართ თქვენი Facebook ანგარიშის მონაცემებით. წმინდა სტატისტიკური თვალსაზრისითაც კი, ეს ზრდის თქვენი ანგარიშის გატეხვის შანსებს. აგრეთვე Facebook-ს საშუალებას აძლევთ, წვდომა მიიღოს თქვენს კიდევ უფრო მეტ პერსონალურ მონაცემზე. ამიტომ, ნურასოდეს შეხვალთ სხვა ვებსაიტებზე თქვენი სოციალური ქსელების ანგარიშების მეშვეობით.

9. იცოდეთ, როგორ უნდა მართოთ საჯაროდ ხელმისაწვდომი და საზიარო მოწყობილობები

სოციალური მედიის ანგარიშებში საჯარო ან საზიარო მოწყობილობებიდან შესვლა ყოველთვის საფრთხეს უქმნის თქვენს პირად ინფორმაციას. მიუხედავად იმისა, რომ თქვენ შეგიძლიათ მინიმუმამდე დაიყვანოთ ზოგიერთი რისკი, მათ ბოლომდე მაინც ვერ აღმოფხვრით. როდესაც იყენებთ საჯარო მოწყობილობას სამსახურში, კაფეში, სკოლაში ან აეროპორტში, თქვენი სოციალური მედიის პროფილების შესამოწმებლად, დარწმუნდით იმაში, რომ მუშაობის დასრულების შემდეგ, სრულად გამოდიხართ სისტემიდან, როდესაც ეს შესაძლებელია, დაასრულეთ სესია ან გადატვირთეთ მოწყობილობა.

შეეცადეთ არ შეხვიდეთ თქვენი სოციალური მედიის ანგარიშებზე ინტერნეტ-კაფეების საერთო კომპიუტერებიდან. ყოველთვის ივარაუდეთ, რომ ასეთ კომპიუტერებზე დაინსტალირებულია keylogger-ები ანუ პაროლის გამხსნელი, ან სხვა ტიპის ჯაშუშური პროგრამები. თუ თქვენი ანგარიში აუცილებლად ინტერნეტ-კაფეში უნდა შეამოწმოთ, დარწმუნდით, რომ ჩართული გაქვთ ორნაბიჯიანი ავტორიზაცია. როგორც კი ანგარიშზე სხვა კომპიუტერიდან შეხვალთ, აუცილებლად შეცვალეთ პაროლი.

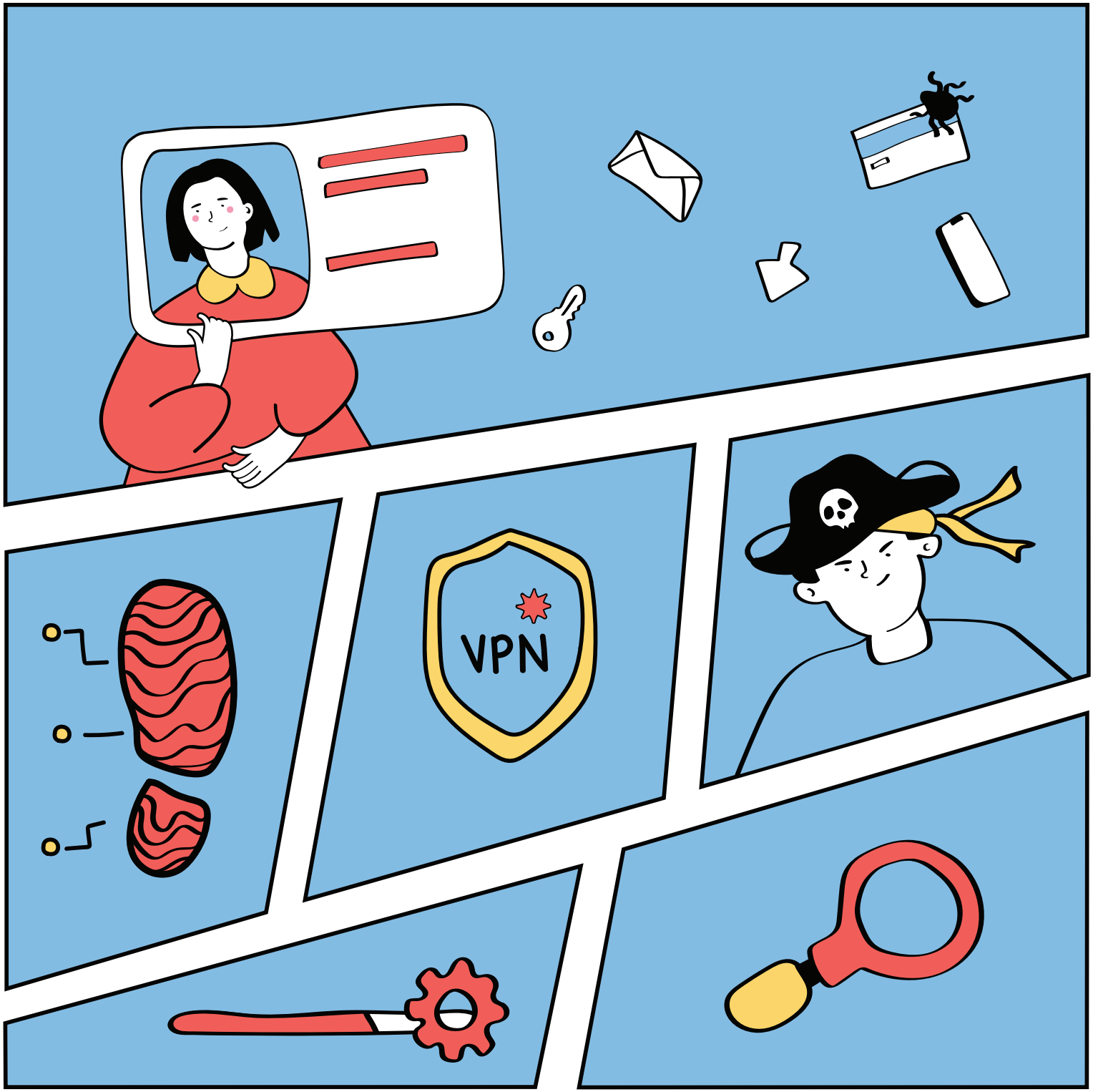
10. უფრთხილდით ბმულებს

ციფრული უსაფრთხოების ერთ-ერთი მთავარი წესია, რომ არასოდეს დააჭიროთ იმ ადამიანების მიერ გამოგზავნილ ბმულებს, ვისაც არ იცნობთ ან ბოლომდე არ ენდობით. ეს ეხება სოციალურ ქსელებში გამოგზავნილ ბმულებსაც. ასეთი ბმულები შეიძლება შეგხვდეთ შემოსულ შეტყობინებებში, ან ფოტოს თუ სტატუსის ქვეშ კომენტარებში. თუ არ იცით ზუსტად, სად გადაგიყვანთ ბმული, არ დააჭიროთ მას.

11. დახურეთ ანგარიშები, რომლებსაც არ იყენებთ

ახალი და მოდური სოციალური მედიის პლატფორმები ანაცვლებს მოძველებულს. ამიტომ მნიშვნელოვანია, დააკვირდეთ თქვენს ყველა ანგარიშს და წაშალოთ ისინი, რომლებსაც აღარ იყენებთ. ჰაკერებისთვის უფრო ადვილია თქვენი მიტოვებული ან დავიწყებული ანგარიშების გატეხვა. ისე, რომ თქვენ ამას ვერც კი შეამჩნევთ.

გატეხილი ანგარიში და მასში არსებული ნებისმიერი ინფორმაცია შეიძლება გამოიყენონ სხვა ანგარიშების გასატეხად. ან იმისთვის, რომ „თქვენგან“ ყალბი ანგარიში შექმნან. გარდა იმ ანგარიშების დახურვისა, რომლებსაც აღარ იყენებთ, სთხოვეთ სოციალური მედიის სერვისებს, სადაც ეს შესაძლებელია, წაშალონ ყველა ინფორმაცია, რომელიც მათ აქვთ თქვენს შესახებ.


VPN