პერსონალურ მონაცემთა
დაცვის ინსპექტორის აპარატი

რეკომენდაციები

ინტერნეტ სივრცეში პერსონალურ მონაცემთა დაცვის შესახებ

ინტერნეტ მომხმარებლებისთვის

დოკუმენტი შემუშავებულია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის, მონაცემთა დაცვის ევროპული სტანდარტებისა და საერთაშორისო პრაქტიკის ანალიზის საფუძველზე. დოკუმენტი სარეკომენდაციო ხასიათისაა. მისი მიზანია, მოქალაქეებს განუმარტოს უფლება-მოვალეობები და ინტერნეტ სივრცეში პერსონალური მონაცემების შემცველი ინფორმაციის გამოყენებისას გასათვალისწინებელი მნიშვნელოვანი გარემოებები.

შესავალი

თანამედროვე ეპოქაში ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა. მისი საშუალებით უამრავი ადამიანი ახორციელებს კომუნიკაციას, ელექტრონულ შესყიდვებს, იღებს სხვადასხვა სახის მომსახურებას, იხდის გადასახადებს, აწარმოებს ოფიციალურ თუ არაოფიციალურ კორესპონდენციას. ელექტრონული კომუნიკაციის საშუალებების განვითარება, სახელმწიფო და საბანკო სერვისების ელექტრონულ სივრცეში გადატანა, ასევე, სოციალური ქსელების პოპულარობა განაპირობებს პერსონალური მონაცემების დიდი მოცულობით დაგროვებას ინტერნეტში.

აღნიშნულ პროცესებში, პერსონალურ მონაცემთა არასათანადო დაცვა ზრდის მონაცემთა დანაშაულებრივი მიზნებისათვის გამოყენების რისკებს და საფრთხის ქვეშ აყენებს ინტერნეტის მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობას. ამიტომ, მნიშვნელოვანია, რომ მოქალაქეებს ჰქონდეთ ინფორმაცია ინტერნეტ სივრცის გამოყენებასთან დაკავშირებული რისკების და მათი უფლებების დაცვის შესახებ.

წინამდებარე რეკომენდაცია განკუთვნილია ინტერნეტ მომხმარებლებისთვის და ითვალისწინებს სახელმძღვანელო წესებს ინტერნეტში პირადი ინფორმაციის დაცვის, უსაფრთხოების ზომების და პერსონალურ მონაცემთა დაცვის კუთხით კანონმდებლობით განსაზღვრული უფლებებისა და ვალდებულებების შესახებ.

სახელმძღვანელო წესები ინტერნეტ მომხმარებელთათვის

ისევე როგორც რეალურ სამყაროში, ვირტუალურ სივრცეშიც ადამიანებს აქვთ უფლებები და მოვალეობები. როდესაც ინტერნეტ მომხმარებელი რეგისტრირდება ვებგვერდზე, იძენს პროდუქტს ან იღებს გარკვეულ მომსახურებას, ის სამართლებრივ ურთიერთობაში შედის ინტერნეტ მომსახურების მიმწოდებელთან და აქვს საშუალება, იზრუნოს საკუთარი პერსონალური მონაცემების დაცვაზე და პირადი ინფორმაციის გამჟღავნების ან უკანონო დამუშავების შემთხვევაში, გამოიყენოს სამართლებრივი მექანიზმები დარღვეული უფლებების აღსადგენად.

ნებისმიერი პირი, რომელიც სარგებლობს ინტერნეტით, მათ შორის ვებგვერდის ავტორიზებული/არაავტორიზებული მომხმარებელი, ინტერნეტ მომსახურების მიმღები (აბონენტი), პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მიხედვით წარმოადგენს მონაცემთა სუბიექტს და მასზე ვრცელდება აღნიშნული კანონის მე-4 თავით გათვალისწინებული უფლებები.

მომხმარებელმა უნდა იცოდეს, რომ ინტერნერტში განხორციელებული თითოეული მოქმედება ტოვებს კვალს. მაგალითად, ვებგვერდზე ვიზიტი, ონლაინ რეგისტრაცია, გაზიარებული ფოტო, ინტერნეტ შესყიდვა და სხვა მრავალი აქტივობა ყოველთვის ფიქსირდება და აღირიცხება. ინტერნეტ მომხმარებელთა მხრიდან ამ გარემოების გათვალისწინება მნიშვნელოვანია, რადგან პერსონალური მონაცემების შემცველი ინფორმაცია (მომხმარებლის ინფორმირების გარეშე) შესაძლებელია, სხვა მიზნითაც იქნას გამოყენებული ინტერნეტ მომსახურების გამწევის მიერ.

! ინტერნეტ სივრცეში არაინფორმირებულმა და გაუაზრებელმა ქმედებამ შესაძლოა საფრთხე შეუქმნას მომხმარებლის პირადი ცხოვრების ხელშეუხებლობას. ხოლო, ინტერნეტ მომხმარებლის მხრიდან გამოჩენილი ყურადღება და სიფრთხილე მნიშვნელოვნად ამცირებს კონფიდენციალური ინფორმაციის გამჟღავნებასთან დაკავშირებულ საფრთხეს. სათანადო უსაფრთხოების ზომების გატარებითა და დაცული ტექნოლოგიური საშუალებებით შესაძლებელია პერსონალური მონაცემების უკანონო გამოყენებასთან დაკავშირებული რისკების შემცირება.

1.1. ზოგადი წესები

ინტერნეტში ნებისმიერი სახის მოქმედების განხორციელებისას მიზანშეწონილია, მომხმარებელი დაინტერესდეს შემდეგი ინფორმაციით:

- ვინ ამუშავებს (აგროვებს, ინახავს, ცვლის და ა.შ.) მის შესახებ მონაცემებს?
- რამდენად აუცილებელია კონკრეტული მონაცემის მიწოდება?
- როგორ მოხდება ამ მონაცემების გამოყენება და რა შედეგი მოჰყვება მას?

განსაკუთრებული სიფრთხილეა საჭირო, როდესაც მომხმარებლისგან ითხოვენ საბანკო ანგარიშებისა თუ საკრედიტო ბარათების შესახებ ინფორმაციას.

ინტერნეტ შესყიდვებისთვის რეკომენდებულია მხოლოდ სანდო ვებგვერდების გამოყენება, რომლებსაც ვებნავიგატორის მისამართების პანელში ერთვის ბოქლომის სიმბოლო, რაც მიუთითებს ტრანზაქციების დაცულობაზე. მიზანშეწონილია, მომხმარებელმა წინასწარ მოიძიოს ინფორმაცია ვებგვერდის და რეალიზატორის შესახებ.

სასურველია, მონაცემების დაცვის მიზნით მომხმარებელმა გამოიყენოს უნიკალური და რთული, მრავალფეროვანი სიმბოლოების კომბინაციისგან შემდგარი პაროლი. მაღალი რისკის შემცველია ერთი და იგივე მომხმარებლის სახელისა და პაროლის გამოყენება სხვადასხვა ინტერნეტ რესურსით სარგებლობისას. იმ შემთხვევაში, თუ ყველა ონლაინ მომსახურების მიღებისას გამოიყენება იდენტური მომხმარებლის სახელი და პაროლი, ერთ-ერთ ანგარიშზე უნებართვო წვდომის შემთხვევაში, მომხმარებლის სხვა ანგარიშებიც დგება საფრთხის ქვეშ.

ყველაზე ხშირად პერსონალური მონაცემების შეგროვება, შენახვა და შემდგომი გამოყენება ხდება მონაცემთა სუბიექტის თანხმობის საფუძველზე. თანხმობას წარმოადგენს ვებგვერდზე რეგისტრაციისას მომხმარებლის მიერ სპეციალური ველის მონიშვნა, რომელშიც მოცემულია ინფორმაცია მომხმარებლის პერსონალურ მონაცემთა გამოყენების წესების შესახებ. მნიშვნელოვანია, რომ ინტერნეტ მომხმარებლები მათ შესახებ ინფორმაციის დამუშავებაზე თანხმობის გამოხატვამდე გაეცნონ ინფორმაციას ინტერნეტ მომსახურების გამწევის მიერ მონაცემთა დამუშავების წესების შესახებ, რომელიც, როგორც წესი, მოცემულია კონფიდენციალურობის შესახებ განაცხადში (Privacy Policy).

1.2. ინფორმაციის მიღების უფლება

ინტერნეტ მომხმარებელს უფლება აქვს ინტერნეტ მომსახურების გამწევისგან მიიღოს ინფორმაცია მისი მონაცემების დამუშავების თაობაზე. კერძოდ:

- რა სახის მონაცემები მუშავდება მის შესახებ, რა არის მათი დამუშავების მიზანი და სამართლებრივი საფუძველი;
- მონაცემთა შეგროვების წყარო;
- ხდება თუ არა მონაცემთა მესამე პირებზე გაცემა, გაცემის საფუძველი და მიზანი.

აღნიშნული ინფორმაცია ან მისი ნაწილი, შესაძლოა მოცემული იყოს კონფიდენციალურობის განაცხადში, წინააღმდეგ შემთხვევაში, მომხარებელს უფლება აქვს, მიმართოს გვერდის ადმინისტრატორს და მოითხოვოს ინფორმაცია.

1.3. მონაცემების გასწორების, შეცვლის და წაშლის მოთხოვნის უფლება

ინტერნეტ მომხმარებელს უფლება აქვს მოითხოვოს მისი მონაცემების წაშლა თუ ისინი არასწორია, ან თუ ამ მონაცემების გამოყენების მიზანი აღარ არსებობს. ინტერნეტ მომსახურების გამწევი კი ვალდებულია დაუყოვნებლივ ან გონივრულ ვადაში შეასრულოს აღნიშნული მოთხოვნა, თუ ადგილი არ აქვს ინტერნეტ მომხმარებლის უფლების შეზღუდვის საფუძველს. *მაგალითად, ინტერნეტ შესყიდვებისათვის განკუთვნილ ვებგვერდზე მომხმარებლის მიერ საკუთარი ანკეტის გაუქმების შემთხვევაში, გვერდის ადმინისტრატორს უფლება აღარ აქვს დაამუშავოს მონაცემები მომხმარებლის მიერ განხორციელებული შესყიდვებისა და ტრანზაქციების შესახებ.*

თუ ინტერნეტ მომხმარებელი ჩათვლის, რომ ინტერნეტ მომსახურების გამწევი ამუშავებს მცდარ, არაზუსტ, მოძველებულ ინფორმაციას, მას აქვს უფლება მოითხოვოს ამ მონაცემების გასწორება, განახლება, დამატება, წაშლა ან განადგურება. მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სუბიექტის განცხადების საფუძველზე, 15 დღის ვადაში, მიიღოს შესაბამისი ზომები და აცნობოს მას მიღებული გადაწყვეტილების შესახებ. *მაგალითად, თუ მომხმარებელი შეიცვლის საცხოვრებელ ადგილს, მას შეუძლია მოსთხოვოს მონაცემთა დამმუშავებელს ძველი მისამართის ახლით ჩანაცვლება.*

1.4. „მზა ჩანაწერები“

„მზა ჩანაწერი“ („Cookies”) ტექსტური ფაილია, რომელიც ავტომატურად იქმნება ვებგვერდზე ვიზიტის, მასზე არჩეული პარამეტრების, განთავსებული სარეგისტრაციო ინფორმაციის და ისტორიის (მაგალითად, ხშირად ნანახი პროდუქციის შესახებ) შესანახად. „მზა ჩანაწერების“ საშუალებით ხდება მომხმარებლის მიერ მოძიებული ინფორმაციისა და ვებგვერდების დამახსოვრება, მომხმარებლის ქცევის და ინტერესების შესწავლა და აღნიშნულზე დაფუძნებით მისთვის სასურველი პროდუქტების/სერვისების ავტომატურ რეჟიმში შეთავაზება. მაგალითად, Amazon, eBay და სხვა ინტერნეტ მაღაზიები იყენებენ აღნიშნულ ტექნოლოგიას და მომხმარებელს ხშირად სთავაზობენ მისი გემოვნებისა და ინტერესის შესაბამის პროდუქტებს. „მზა ჩანაწერების“ საშუალებით ასევე შესაძლებელია ინტერნეტში მომხმარებლის ნავიგაციის შესახებ ინფორმაციის მიღება. კერძოდ, მათი მეშვეობით დგინდება, თუ რამდენი ხანი დაჰყო მომხმარებელმა ვებგვერდზე და რამდენად ხშირად სტუმრობს კონკრეტულ გვერდებს. ასევე, შესაძლოა კონკრეტული ვებგვერდი ახდენდეს „მზა ჩანაწერების“ გაზიარებას სხვა გვერდებისთვის, რაც მნიშვნელოვნად ამცირებს მომხმარებლის მხრიდან საკუთარი ინფორმაციის კონტროლის შესაძლებლობას.

ინტერნეტ მომხმარებელს აქვს საშუალება, ვებნავიგატორის მენიუში არსებული კონფიდენციალურობის პარამეტრების გამოყენებით, არ მისცეს ვებგვერდებს „მზა ჩანაწერების“ შექმნის და გამოყენების უფლება. ვებნავიგატორის მენიუში არსებობს „მზა ჩანაწერების“ მარეგულირებელი სპეციალური ფუნქცია, რომელიც საშუალებას აძლევს მომხმარებელს, აკონტროლოს ინფორმაციული ნაკადების გადინება მისი მოწყობილობიდან (კომპიუტერი, ტაბლეტი, მობილური).

კონფიდენციალურობის პარამეტრების გამოყენებით მომხმარებელს შეუძლია, წაშალოს მზა ჩანაწერი, დაბლოკოს მზა ჩანაწერის შექმნის შესაძლებლობა ან ავტომატურ რეჟიმში მოახდინოს სისტემიდან გამოსვლის დროს მზა ჩანაწერის წაშლა. ასევე, შესაძლებელია კონფიდენციალური ვებნავიგაციით სარგებლობა, რომელიც არ ინახავს ისტორიას და არ იმახსოვრებს თავდაპირველ ჩანაწერებს.

1.5. თაღლითური სქემები

ინტერნეტში არსებობს საკმაოდ ბევრი, სხვადასხვა ტიპის თაღლითური ვებგვერდი, რომელიც ერთი შეხედვით საკმაოდ უსაფრთხოდ შეიძლება გამოიყურებოდეს. აღნიშნული ვებგვერდები ხშირად ითხოვენ საბანკო ანგარიშებისა და საკრედიტო ბარათების შესახებ ინფორმაციას. თაღლითური სქემების ნაწილია ასევე ე.წ. საეჭვო ელექტრონული წერილები (Spam E-mail), რომლებიც ელ-ფოსტის მისამართების შემთხვევითი შერჩევის გზით მილიონობით ადრესატს ეგზავნება. *მაგალითად, ელექტრონული შეტყობინება ლატარიაში გამარჯვების ან ფულადი თანხის მოგების შესახებ.* მსგავსი სახის წერილები ხშირად ვირუსული ხასიათისაა ან/და იძლევა ინტერნეტ მომხმარებლის მონაცემების არამართლზომიერი მოპოვების საშუალებას. ისინი შესაძლებელია საფრთხეს უქმნიდეს მოწყობილობას ან/და მასში დაცულ დოკუმენტებს, საბანკო მონაცემებს, პაროლებს და სხვა).

როგორც წესი, თაღლითურ ვებგვერდებს არ აქვთ მითითებული საკონტაქტო ინფორმაცია, არ გააჩნიათ კონფიდენციალობის განაცხადი, მომხმარებელს სთავაზობენ გაურკვეველი ტიპის ფაილების ავტომატურ რეჟიმში გადმოტვირთვას, შეიცავენ ცრუ „ახალ ამბებს“, საეჭვო ტიპის სარეკლამო ბანერებს და ა.შ. გარდა ამისა, თაღლითმა შეიძლება მიითვისოს და უკანონოდ გამოიყენოს თქვენი პირადი ინფორმაცია (ე.წ. Identity Theft). საკმაოდ გავრცელებულია თაღლითების მიერ დაზარალებულის საიდენტიფიკაციო ნომრისა და დაბადების თარიღის გამოყენებით ახალი საკრედიტო ანგარიშის გახსნა და ბარათის გამოყენება, ასევე, ტელეფონის, ინტერნეტისა და სხვა კომუნალური მომსახურებების გადასახადის გაფორმება დაზარალებულის სახელზე ან დავალიანების დაფარვა დაზარალებულის ანგარიშიდან.

პერსონალური მონაცემების დაცვის მიზნით სასურველია, რომ ინტერნეტ მომხმარებელი:

- ელექტრონული ფოსტის სერვისზე რეგისტრაციის დროს ეცნობოდეს კონფიდენციალობის პირობებს;
- ერთმანეთისგან მიჯნავდეს სამსახურებრივ და პირად კორესპონდენციას და აწარმოებდეს მათ სხვადასხვა ელექტრონული ფოსტის მისამართიდან;
- თავს იკავებდეს საეჭვო ტიპის შეტყობინებების და მასზე მიმაგრებული ფაილების გახსნისგან, ასევე, მსგავს შეტყობინებებზე პასუხის გაცემისგან;
- იყენებდეს ფილტრაციის ფუნქციას. მონიშნოს, რომ შეტყობინება საეჭვო ფოსტას (Spam email) განეკუთვნება, რათა თავიდან აიცილოს მათი შემდგომში მიღება ან ძირითად წერილებთან ერთად მოხვედრა;
- სხვადასხვა ვებგვერდებზე რეგისტრაციამდე (მაგალითად, ონლაინ მაღაზიები ან სიახლეების გამოწერა) აფასებდეს მათ სანდოობას და ეცნობოდეს კომპანიის კონფიდენციალურობის პირობებს;
- იყენებდეს ანტივირუსის პროგრამას.

1.6. სოციალური ქსელები

სოციალური ქსელებს (მაგალითად Facebook, Twitter, Instagram, LinkedIn და სხვა) ყოველდღიურად მილიონობით ადამიანი იყენებს. ნებისმიერი სახის სოციალური ქსელში მომხმარებელი კარგავს კონტროლს მის მიერ გაზიარებულ ინფორმაციაზე, რაც საფრთხეს უქმნის პერსონალური მონაცემების კონფიდენციალურობასა და პირად ცხოვრებას.

სოციალურ ქსელში ინფორმაციის გამჟღავნებამდე სასურველია, რომ მომხმარებელი ყურადღებით მოეკიდოს შემდეგ გარემოებებს:

- **მონაცემების გასაჯაროების ფარგლები.** სოციალური ქსელების უმრავლესობას აქვს ფუნქცია, რომლის დახმარებითაც მომხმარებელს შეუძლია, გააკონტროლს თუ ვის უზიარებს მის მიერ გამოქვეყნებულ ინფორმაციას. ვებგვერდზე არსებული კონფიდენციალურობის პარამეტრები იძლევა გაზიარებულ ინფორმაციაზე წვდომის შეზღუდვის შესაძლებლობას. მაგალითად, აღნიშნული პარამეტრების გამოყენებით შესაძლებელია ფოტოს გაზიარება მხოლოდ პირთა ვიწრო წრისთვის.

- **თაღლითური სქემები.** თაღლითები ხშირად იყენებენ სოციალურ ქსელებში ხელმისაწვდომ ინფორმაციას. ამიტომ მომხმარებელმა მაქსიმალურად უნდა შეიკავოს თავი სოციალურ ქსელში ისეთი ინფორმაციის განთავსებისგან, როგორიცაა პირადი ნომერი, პასპორტის მონაცემები და ა.შ.

- **საეჭვო ჯგუფები.** ასეთი ჯგუფების მეშვეობით ხშირად ვრცელდება ცრუ ინფორმაცია და მავნე კოდის შემცველი ბმულები.

- **მესამე პირთა ინფორმაციის გამჟღავნება.** სხვა პირთა პირადი ინფორმაციის გაზიარებამდე მიზანშეწონილია მომხმარებელმა მიიღოს მათი თანხმობა.

სოციალურ ქსელებს კონფიდენციალურობის და პერსონალური მონაცემების დაცვის განსხვავებული ფუნქციები და შესაძლებლობები აქვთ. *ცხრილში მოცემულია რამდენიმე პოპულარული ქსელის ფუნქციების შესახებ ინფორმაცია.*

	facebook	twitter	LinkedIn	Google+
რეგისტრაციის დროს თქვენი პროფილის ხილვადობის შეზღუდვა	√	X	X	X
თქვენი პროფილის ძებნის კონტროლი	√	√	√	X
თქვენთან დაკავშირების/დამეგობრების მსურველთა წრის შეზღუდვა	√	X	√	X
თქვენთვის შეტყობინების გამოგზავნის შესაძლებლობის შეზღუდვა	√	X	√	√
თქვენი მეგობრების (კავშირების) ნახვის შეზღუდვა	√	X	√	√
განცხადებებზე (“პოსტებზე“) თქვენი მონიშვნის შესაძლებლობის შეზღუდვა	√	X	X	X
თქვენი ფოტოების მნახველთა წრის შეზღუდვა	√	X	√	√
არასასურველი პირის დაბლოკვის შესაძლებლობა	√	√	√	√
ფოტო-მონიშვნის კონტროლი	X	√	-	X
სახის ამომცნობი სისტემის გამორთვა	√	-	-	√
საძიებო სისტემებში თქვენი პროფილის ხელმისაწვდომობის შეზღუდვა	√	X	X	√
ბოლო დროს განხორციელებული წვდომების ნახვა	√	X	X	√
პროფილზე შესვლის დროს ტექსტური ან ხმოვანი შეტყობინების დაყენება	√	X	X	√
ორდონიანი იდენტიფიცირების მხარდაჭერა	√	√	√	√
უსაფრთხო კავშირის მხარდაჭერა (SSL)	√	√	X	√
აპლიკაციების კონტროლი	√	√	√	√
მესამე პირის აპლიკაციებისთვის მონაცემთა გადაცემის შეზღუდვა	√	X	X	X
ადგილმდებარეობის მაჩვენებლის გამორთვა	√	√	-	√
ადგილმდებარეობის მონაცემების წაშლა	√	√	X	√
რეკლამების კონტროლი	√	X	X	X
სარეკლამო შეთავაზებებზე უარის თქმა	X	X	X	X
თქვენი პერსონალური ინფორმაციის გამოთხოვა	√	√	√	√
პროფილის წაშლა	√	√	√	√

1.7. ღრუბელი

ყოველდღიურად იზრდება ღრუბლოვანი (მაგალითად, Dropbox, GoogleDrive, iCloud) მომსახურების მომხმარებლთა რაოდენობა. ღრუბელი ელექტრონულ რესურსებზე საყოველთაო და მოხერხებული ქსელური წვდომის მრავალფუნქციური მოდელია, რომელზეც მომხმარებელს შეუძლია, სხვებისთვის გაზიარების ან შენახვის მიზნით ატვირთოს დოკუმენტები, სურათები, ვიდეო ან აუდიოჩანაწერები. ატვირთულ ინფორმაციაზე წვდომა შესაძლებელია ნებისმიერი ადგილიდან და ნებისმიერი მოწყობილობიდან (ლეპტოპი, სმარტფონი, პერსონალური კომპიუტერი და ა.შ.). ამისთვის მხოლოდ ქსელთან კავშირია საჭირო.

! ნებისმიერი წვდომის სახის არჩევის შემთხვევაში მომხმარებელს უნდა ახსოვდეს, რომ მონაცემების ნახვის შესაძლებლობა ღრუბლის მწარმოებელ კომპანიასაც აქვს.

გასათვალისწინებელია, რომ ღრუბლის მომსახურების მიმწოდებელი მხოლოდ ატვირთული ინფორმაციის შენახვაზეა პასუხისმგებელი. ამიტომ მნიშვნელოვანია, მომხმარებელი გაეცნოს პერსონალური მონაცემების დაცვის და უსაფრთხოების პარამეტრებს და დარწმუნდეს, რომ ისინი შეესაბამება ღრუბელზე განთავსებული ინფორმაციის კონფიდენციალურობის ხარისხს.

ღრუბლის და მსგავსი სახის მომსახურებებების გამოყენებისას მნიშვნელოვანია, რომ მომხმარებელმა განსაზღვროს ვის შეიძლება ჰქონდეს წვდომა მის მიერ განთავსებულ ინფორმაციასთან.

არსებობს წვდომის სამი ძირითადი სახე:

1. **პირადი**. მონაცემების მესაკუთრის გარდა არავის აქვს მათი ნახვის უფლება.
2. **საზიარო**. მომხმარებელს შეუძლია, გაუზიაროს განთავსებული ინფორმაცია სასურველ პირებს შესაბამისი შეტყობინებისა და წვდომის ბმულის გაგზავნის გზით.
3. **საჯარო**. განთავსებული ინფორმაციის ნახვა შეუძლია ნებისმიერ მსურველს.

ღრუბელზე განთავსებული ინფორმაციის დაცვა მონაცემების დაშიფვრითაც არის შესაძლებელი. ასეთ შემთხვევაში შეუძლებელი იქნება ინფორმაციის ნახვა ან შეცვლა შესაბამისი შიფრის გასაღების გარეშე. დაშიფრვა ხორციელდება მომხმარებლის მიერ საკუთარი ელექტრონული მოწყობილობის (კომპიუტერი, სმარტფონი) პროგრამული უზურუნველყოფის მეშვეობით და შესაბამისად, დაშიფვრისათვის აუცილებელი გასაღების დაცულობასა და უსაფრთხოებაზე პასუხისმგებელი თავად მომხმარებელია.

1.8. არასრულწლოვანთა უფლებების დაცვა

განსაკუთრებულ ყურადღებას მოითხოვს არასრულწლოვანთა მიერ ინტერნეტის გამოყენების საკითხი. თანამედროვე რეალობაში, ბავშვები უფრო მეტად იყენებენ ონლაინ რესურსებს, ვიდრე მათი მშობლები თუმცა, ხშირად, ისინი სათანადოდ ვერ აფასებენ მონაცემთა გამჟღავნებასთან და თაღლითურ სქემებთან დაკავშირებულ საფრთხეებს, სწორედ ამიტომ:

- თვალყური ადევნეთ თქვენი შვილების ქცევას ონლაინ სივრცეში და მიეცით მათ უსაფრთხოების შესახებ რჩევები;
- აუხსენით ბავშვებს, რომ არ უნდა განათავსონ ინტერნეტში ისეთი მონაცემები, როგორიცაა სახლის მისამართი, ტელეფონის ნომერი, პაროლი და სხვა;
- განუმარტეთ მათ, რომ ქსელში უცნობ ადამიანებთან კომუნიკაცია სახიფათოა (უცნობი შეიძლება იტყუებოდეს და მალავდეს რეალურ ასაკს, ვინაობას). აუხსენით ბავშვებს, რომ დაუშვებელია თქვენი თანხმობისა და მეთვალყურეობის გარეშე ინტერნეტ სივრცის გარეთ უცნობ ადამიანებთან შეხვედრა;
- დაარწმუნეთ ბავშვები, რომ არ უნდა გახსნან უცხო პირებისგან მიღებული ელექტრონული წერილები და ბმულები, რადგან ისინი შეიძლება შეიცავდეს ვირუსს ან მავნე კოდს;
- თუ თქვენი შვილები იყენებენ სოციალურ ქსელებს, შეამოწმეთ კონფიდენციალურობისა და უსაფრთხოების პარამეტრები;
- გააფრთხილეთ ბავშვები, რომ სხვისი ელექტრონული მოწყობილობის გამოყენებისას არ უნდა მონიშნონ მომხმარებლის/პაროლის დამახსოვრების ველი (remember me/remember password) და უნდა გამოვიდნენ პროგრამიდან/ქსელიდან (log out) მისი გამოყენებისთანავე;

სპეციალური პროგრამების გამოყენებით შესაძლებელია გარკვეულ ვებგვერდებზე წვდომის შეზღუდვა და ინტერნეტ სივრცეში თქვენი შვილების აქტივობების კონტროლი.

1.9. გასაჩივრების უფლება

ინტერნეტ მომსახურების გამწევის მხრიდან მონაცემთა არამართლზომიერ გამოყენების შემთხვევაში, დიდი მნიშვნელობა ენიჭება მომხმარებლების მიერ, საკუთარი უფლებების დაცვის ეფექტური საშუალებების არსებობას. იმ შემთხვევაში, თუ ინტერნეტ მომსახურების გამწევი დაარღვევს პერსონალურ მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებულ უფლებებს, მომხმარებლებს უფლება აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი წესით მიმართონ პერსონალურ მონაცემთა დაცვის ინსპექტორს ან სასამართლოს.

თუ კი სახეზეა კიბერდანაშაული, კერძოდ მოხდა თქვენ კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა, სასწრაფოდ მიმართეთ სამართალდამცავ ორგანოებს.