ინტერნეტში უსაფრთხოების გზამკვლევი მშობლებისთვის

გაძლივ იავიჩი
გიორგი იაშვილი

2020 წელი

World Vision

სარჩევი

რა უნდა ვიცოდეთ ინტერნეტის შესახებ?

დღეს ბავშვები ინტერნეტით აღჭურვილ სამყაროში იბადებიან. ციფრული სამყარო მათი არსებობის ყველა ასპექტს მოიცავს: ეს იქნება სწავლა, თამაში, მეგობრებთან კომუნიკაცია, თუ მნიშვნელოვანი მომენტების ამსახველი ფოტოები.

მნიშვნელობა არ აქვს სახლში იმყოფებიან, სკოლაში, თუ მეგობართან, ბავშვები მუდმივად არიან ჩართულნი ინტერნეტში, რაც შესაძლოა მშობლების შეშფოთებასაც კი იწვევდეს. რა თქმა უნდა ინტერნეტი მნიშვნელოვან როლს ასრულებს განათლების მიღების პროცესში, ვინაიდან ბავშვებს შეუძლიათ მისი გამოყენება სასკოლო დავალებების დასაწერად, მასწავლებლებთან და სხვა ბავშვებთან ურთიერთობისთვის, ინტერაქტიული თამაშებისთვის და სხვა.

მაგრამ ყველა სიკეთესთან ერთად ციფრულმა ტექნოლოგიებმა ბავშვები კიდევ უფრო დიდი საფრთხის წინაშე დააყენა. პრობლემებმა, რასაც ბავშვები რეალურ ცხოვრებაში აწყდებოდნენ, მაგალითად, ბულინგი, ძალადობა და ა.შ. ინტერნეტ სივრცეში გადაინაცვლა და შეიძლება ითქვას, მოიმატა კიდეც, რადგან, თუ ბავშვებს ინტერნეტთან წვდომა აქვთ, ყველაზე დაცულ ადგილზეც კი, (მაგალითად სახლში) არ არიან უსაფრთხოდ.

რა უნდა ვიცოდეთ ინტერნეტის შესახებ?

ასეთ საფრთხეებთან გამკლავება მხოლოდ ცოდნით არის შესაძლებელი, უპირველეს ყოვლისა მშობლებმა და მასწავლებლებმა უნდა იცოდნენ, თუ რა საფრთხეები არსებობს ინტერნეტში და როგორ უნდა დაიცვან მათგან თავი, რომ შეძლონ ბავშვის ინფორმირება და დახმარება. ეს არ არის ერთჯერადი აქტივობა, ეს არის პროცესი, რომელიც მოითხოვს მუდმივ ურთიერთობასა და მუშაობას ბავშვთან, დიდ მოთმინებას და ენერგიას, რისთვისაც ყველა მშობელი უდნა იყოს მზად.

მშობელი უნდა დაეხმაროს ბავშვს ინტერნეტში მუშაობისათვის საჭირო უნარების განვითარებაში, ინტერნეტით მიღებული მასალებისა და კონტაქტების სანდოობის შემოწმებასა და კრიტიკულად გააზრებაში. ბავშვმა უნდა შეძლოს ინტერნეტიდან მომავალი საფრთხეების დროულად ამოცნობა და საჭიროების შემთხვევაში მშობლისა და პედაგოგისათვის მიმართვა.

ინტერნეტის გამოყენების საფრთხეები

ბავშვების მიერ ინტერნეტის გამოყენება არაერთ საფრთხესთანაა დაკავშირებული, როგორც უკვე ითქვა, მათ ჯერ კიდევ არ აქვთ გამომუშავებული კრიტიკული აზროვნების უნარი და შეიძლება ბრმად ენდონ ინტერნეტით გაცნობილ ნებისმიერ პირს ან მიღებულ ინფორმაციას. სწორედ ამ გარემოებას იყენებენ კიბერ დამნაშავეები თავიანთი ზრახვების განსახორციელებლად. ისინი ადვილად ახერხებენ ბავშვებთან ურთიერთობის დამყარებას სოციალური მედიის ანონიმური ანგარიშების, ონლაინ თამაშების, ჩატების ან ფორუმების საშუალებით, მაშინ, როცა ბავშვი ცუდს არაფერს ეჭვობს. დამნაშავემ შეიძლება ბავშვის ან მოზარდის ყალბი პროფილი შექმნას და „თანატოლებს“ მეგობრობის მოთხოვნა დაუგზავნოს, შემდგომში მათგან პირადი ინფორმაციის მიღების მიზნით.

გთავაზობთ ინტერნეტიდან მომავალი საფრთხეების რამდენიმე მაგალითს:

კონტაქტი არასასურველ პირებთან:

- **„მტაცებლები“** - ძირითადად გვხვდებიან სოციალური ქსელებში ან ონლაინ თამაშების ჩატებში.

- **კიბერ ხულიგნები** - ბავშვები შეიძლება კიბერ ხულიგნების სამიზნედ იქცნენ, ჩვეულებრივი რეალური ხულიგნების ჩათვლით.

- **ფიშინგ თაღლითები** - ცდილობენ ბავშვებს გამოსტყუონ ინფორმაცია, როგორც საკუთარ თავზე, ასევე მშობლების შესახებ.

ინტერნეტის გამოყენების საფრთხეები

ბავშვებისათვის არასასურველი შინაარსის შემცველი ინფორმაცია:

- **სექსუალური შინაარსის შეტყობინებები** - განსაკუთრებით პორნოგრაფიული სურათები და ვიდეო.

- **ძალადობა** - როგორიცაა სისხლისღვრა ან თავდასხმის აქტები.

- **უხამსი ან ასაკთან შეუსაბამო ქმედება** - მაგალითად, გინება, ნარკოტიკის და ალკოჰოლის გამოყენება.

- **პირატული მასალები და მათი კომიუტერში ჩამოტვირთვით გამოწვეული საფრთხეები** - მუსიკალური ან ვიდეო ფაილების ჩათვლით.

- **ინტერნეტში გავრცელებული ტენდენციები და ე.წ. "გამოწვევები" მოზარდებისათვის - მარილის და ყინულის გამოწვევა, სავსე კოვზი, Neknominate და თამაში გაგუდვა.**

მშობლების ჩართულობას, თავიანთი შვილების ონლაინ ცხოვრებაში შეუძლია მათი დაცვა ინტერნეტიდან მომავალი საფრთხეებისაგან. მაგალითისათვის კიბერბულინგთან დაკავშირებულმა ცნობიერების ზრდამ, ასწავლა მშობლებს, თუ როგორ გაუმკლავდნენ ამ პრობლემას.

რა არის კიბერბულინგი ?

კიბერბულინგი - ბულინგის სახეობა, რომელიც ონლაინ სივრცეში ხორციელდება შეურაცხყოფის შემცველი შეტყობინებებით, აგრესიით, დაშინებით, სხვადასხვა ინტერნეტსერვისების გამოყენებით.

ძირითადად კიბერბულინგის მონაწილე ყველა მხარე უნდა იყოს მოზარდი. თუ მსგავს ქმედებას სრულწლოვანი ახორციელებს, ეს უკვე კიბერდანაშაულია და ზოგიერთ შემთხვევაში პატიმრობასაც კი ითვალისწინებს.

კიბერბულინგის მსხვერპლ მოზარდთა უმრავლესობა თავს არიდებს მომხდარი ინციდენტების გამხელას, რადგანაც რცხვენია სოციალური სტიგმის ან იმის, რომ უფროსები ინტერნეტითა და კომოიუტერით სარგებლობას აუკრძალავენ. ზემოხსენებული ართულებს კიბერბულინგის მსხვერპლთა რეალური რაოდენობის დადგენას, თუმცა ბოლო დროს კიბერშეტევების მაჩვენებლებზე ჩატარებულმა კვლევებმა აჩვენა, რომ დაახლოებით ოთხიდან ერთი თინეიჯერი ხდება კიბერბულინგის მსხვერპლი, ექვსი მოზარდიდან ერთმა კი აღიარა, რომ სხვის მიმართ ჩაუდენია მსგავსი ქმედება.

კიბერბულინგის ნიშნები

კიბერბულინგის ნიშნები განსხვავებულია, თუმცა არსებობს რამდენიმე ძირითადი მახასიათებელი, რომლის საშუალებითაც შეძლებთ მსგავსი შემთხვევის ამოცნობას:

- განწყობის გაფუჭება ინტერნეტის ან ტელეფონის გამოყენების შემდეგ.
- ციფრული ცხოვრების უაღრესად გასაიდუმლოება და დაცვა.
- ოჯახის წევრებთან და მეგობრებთან დისტანციის ზრდა.
- სკოლის ან ჯგუფური შეკრებებისთვის თავის არიდება.
- აკადემიური მოსწრების დაქვეითება და გაბრაზებული ქცევა სახლში.
- განწყობის, ქცევის, ძილის ან მადის ცვლილებები.
- კომპიუტერის ან მობილური ტელეფონის გამოყენების შეწყვეტის სურვილი.
- გაღიზიანება და პანიკური ქცევა შეტყობინებების მიღებისას.
- კომპიუტერთან ან მობილურ ტელეფონთან დაკავშირებული აქტივობების შესახებ დისკუსიების თავიდან აცილება.

მშობლის როლი კიბერბულინგის დროს

თუ აღმოაჩენთ, რომ თქვენი შვილი გახდა კიბერბულინგის მსხვერპლი, დაამშვიდეთ და დახმარება შესთავაზეთ, აუხსენით, რომ ეს მისი ბრალი არ არის და ბულინგი უფრო მეტს მეტყველებს არა მსხვერპლზე, არამედ თავად ბულინგის განმახორციელებელზე. შეაქეთ თქვენი შვილი, უთხარით მას, რომ სწორად იქცევა, როდესაც ამის შესახებ გიყვებათ. შეახსენეთ, რომ მარტო არ არის და ძალიან ბევრი ადამიანი ყოფილა მსგავს სიტუაციაში, დაპირდით, რომ ერთად მონახავთ ამ პრობლემის გადაწყვეტის გზას.

შექმნილი მდგომარეობის შესახებ ესაუბრეთ სკოლის თანამშრომელს.

ბევრ სკოლას აქვს კიბერბულინგზე რეაგირების პროტოკოლი. დაარწმუნეთ ბავშვი რომ არ უპასუხოს კიბერბულინგს, რადგან ეს მხოლოდ ართულებს მდგომარეობას, მაგრამ აუცილებლად შეინახეთ ბულინგის შემცველი შეტყობინებები, ეს შეიძლება მტკიცებულებად გამოგადგეთ ხულიგნის მშობლებთან, მასწავლებელთან და შესაძლოა პოლიციასთანაც კი.

რა დამატებითი ზომების მიღებაა საჭირო ?

შექმნილ ვითარებაში საჭიროა კიბერ ხულიგნის დაბლოკვა. მოწყობილობების უმეტესობას აქვს პარამეტრები, რომლებიც კონკრეტული პირებისგან შემომავალი შეტყობინებების დაბლოკვის საშუალებას იძლევა. უმჯობესია იცოდეთ ასეთი უსაფრთხოების პარამეტრების შესახებ და შეძლოთ მათი გამოყენება.

მშობლის როლი კიბერბულინგის დროს

შეზღუდეთ წვდომა ტექნოლოგიებთან. მიუხედავად იმისა, რომ კიბერბულინგის ქვეშ მყოფი ბავშვები ძლიერი სტრესის მდგომარეობაში იმყოფებიან, მათ მაინც არ შეუძლიათ სძლიონ და არ შეამოწმონ ვებგვერდები ან ტელეფონი ახალი შეტყობინებების სანახავად.

- განათავსეთ კომპიუტერი საერთო სარგებლობის ოთახში (არავითარი ლეპტოპი ბავშვების საძინებელში), დააწესეთ შეზღუდვები ტელეფონის გამოყენებაზე და ინტერნეტ თამაშებზე. ზოგიერთი კომპანია შეტყობინებების გამორთვის საშუალებას გაძლევთ, ხოლო ვებსაიტების და სმარტფონების უმეტესობა აღჭურვილია მშობელთა კონტროლის ელემენტებით, რაც ბავშვების ონლაინ საქმიანობის გაკონტროლების საშუალებას იძლევა.

- დაუმეგობრდით თქვენს შვილს სოციალურ ქსელებში, ან გახდით მისი „გამომწერი“, მაგრამ შეეცადეთ არ განათავსოთ მის გვერდზე ჩანაწერები და კომენტარები. თვალყური ადევნეთ თქვენი შვილის შეტყობინებებს და შეამოწმეთ რომელ საიტებს სტუმრობს. ესაუბრეთ მას კონფიდენციალურობის მნიშვნელობაზე და აუხსენით, თუ რატომ არ შეიძლება პირადი ინფორმაციის გაზიარება ინტერნეტით. ერთად შეიმუშავეთ მობილურის და სოციალური ქსელების გამოყენების წესები, რომელთა შესრულებასაც მოითხოვთ თქვენი შვილისგან.

- იმისათვის, რომ უზრუნველყოთ თქვენი შვილის უსაფრთხოება ინტერნეტში. დაარწმუნეთ ის, რომ მოუფრთხილდეს პაროლებს და არასოდეს გაამჟღავნოს თავისი მისამართი და ადგილმდებარეობა.

- თუ თქვენი შვილი თანახმა იქნება, შეგიძლიათ მიმართოთ თერაპევტს ან სკოლის მრჩეველს.

თუ თქვენი შვილი კიბერ ბულერია

მშობლისთვის ყოველთვის მტკივნეულია, იმის გაგება, რომ მისი შვილი ცუდად იქცევა. მნიშვნელოვანია დაუყოვნებლივ დაიწყოთ მოქმედება პრობლემის გადასაჭრელად და არ დაელოდოთ როდის მოგვარდება იგი თქვენი ჩარევის გარეშე.

- მტკიცედ ელაპარაკეთ თქვენს შვილს და აუხსენით რა უარყოფითი გავლენის მოხდენა შეუძლია სხვებზე მის საქციელს. ხუმრობა ერთისთვის შეიძლება არაფერს ნიშნავდეს, ხოლო მეორესთვის მტკივნეული იყოს. ასეთ საქციელს შეიძლება სერიოზული შედეგები მოჰყვეს სახლში, სკოლაში და საზოგადოებაში.

- დაუწესეთ მოზარდს ლიმიტი მოწყობილობებით სარგებლობაზე და აკონტროლეთ მისი აქტივობა ინტერნეტში.

- საკითხის არსში გასარკვევად შეგიძლიათ მიმართოთ მასწავლებლებს, კონსულტანტებს და სკოლის სხვა წარმომადგენლებს, რომ გაარკვიოთ, თუ რამ აიძულა ასეთი საქციელის ჩადენა. თუ თქვენს შვილს უჭირს აგრესიის კონტროლი, გაესაუბრეთ თერაპევტს და დაეხმარეთ ბავშვს ისწავლოს სიბრაზესთან, წყენასთან, იმედგაცრუებასთან და სხვა ძლიერ ემოციებთან ჯანსაღი წესით გამკლავება. პროფესიონალურ კონსულტაციას ასევე შეუძლია ბავშვის თავდაჯერებულობისა და სოციალური უნარების გაუმჯობესება, რამაც თავის მხრივ შეიძლება საგრძნობლად შეამციროს ბულინგის შესაძლებლობა.

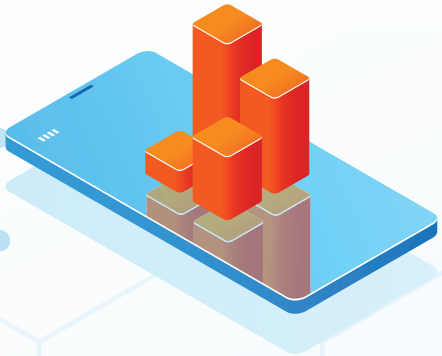
ინტერნეტში გავრცელებული თანამედროვე ტენდენციები

სოციალური ქსელების მზარდი პოპულარობის კვალდაკვალ იმატა მასში უცნაური მოვლენების გავრცელებამ. მსგავსი ქსელები საშუალებას აძლევს მოზარდებს, ფართო აუდიტორიას გაუზიარონ საკუთარი ვიდეოები და ფოტოები, რაც იწვევს მათში მღელვარების შეგრძნებას, ზრდის პატივისცემის დამსახურების, მოწონებებისა და გამომწერთა რაოდენობის გაზრდის დაუოკებელ სურვილს, რაც საბოლოოდ, უბიძგებს ბავშვებს კიდევ უფრო მეტი ინფორმაცია გააზიარონ საკუთარი თავის შესახებ და მეტი დრო გაატარონ ონაილ სივრცეში.

ინტერნეტ გამოწვევების ბნელი მხარე

ბევრი ონლაინ გამოწვევა და პრობლემა უწყინარია, მაგრამ ზოგიერთი მათგანი სერიოზული ტრავმების მიზეზად იქცა, მაგალითად:

მარილის და ყინულის გამოწვევა - ამ გამოწვევაში მონაწილეები სხეულის ნაწილზე იყრიან მარილს და ზემოდან იმაგრებენ ყინულის კუბს. მარილი ამცირებს ყინულის კუბის ტემპერატურას და იწოვს სითბოს კანიდან ყინულის დნობის შესაბამისად. შედეგად კანის ტემპერატურა ბევრად უფრო ძლიერად ეცემა ვიდრე ეს მოხდებოდა მხოლოდ ყინულის გამოყენების შემთხვევაში. ამას შეუძლია სხვადასხვა ტრავმის - მოყინვის, მოუშუშებელი ნაწიბურების გამოწვევა.



ინტერნეტში გავრცელებული თანამედროვე ჭენდენციები

სავსე კოვზი - დარიჩინის შეჭმა და რეაქციის გადაღება. ასეთი ვიდეოს ინტერნეტში ატვირთვა რამდენიმე წლის განმავლობაში ძალიან პოპულარული იყო. ამ გამოწვევაში მონაწილეთა უმეტესობა დღეს თავს კარგად გრძნობს, მაგრამ იყო ცნობები ასთმის შეტევებისა და რესპირატორული პრობლემების შესახებ.

Neknominate - ამ გამოწვევასთან დაკავშირებულია რამდენიმე ლეტალური და ჰოსპიტალიზაციის შემთხვევა, მას შემდეგ, რაც ახალგაზრდებმა მიიღეს დიდი რაოდენობით ალკოჰოლური და სხვა სასმელები.

„თამაში გაგუდვა“ - მონაწილე განზრახ იკეტავს ჟანგბადის მიღების გზებს. ეს გამოწვევა უამრავი ლეტალური შემთხვევის მიზეზი გახდა და მიუხედავად იმისა, რომ ეს თამაში არ არის ახალი, მსგავსი ვიდეოები კვლავ ვრცელდება სოციალურ ქსელებში.

ასევე არსებობს რამდენიმე ვებგვერდი, რომელიც იწვევს „გაბედულებს“. ქულების დაგროვების ცდუნება ბავშვებს უფრო მეტ რისკზე წასვლას აიძულებს. მონაწილეებმა შეიძლება დააწესონ გამოწვევა და მოითხოვონ შესრულებული დავალების ვიდეო ან ფოტო მტკიცებულება. ერთ-ერთ ასეთ საიტზე იყო საგანგაშო შემთხვევებიც, სადაც მონაწილეებს გაშიშვლებას და ვიდეოს გადაღებას სთხოვდნენ. დავალებაში სპეციალურად იყო მითითებული ასაკი 8-12 წელი. ამ საიტების უმეტესობა დღესაც არსებობს, სადაც ათასობით სულელური და საშიში გამოწვევაა გამოქვეყნებული.

ინტერნეტში გავრცელებული თანამედროვე ტენდენციები

რისი გაკეთება შეგიძლიათ ?

ძნელია ბავშვებისთვის ინტერნეტით ხუმრობებში, თამაშებში და გამოწვევებში მონაწილეობის აკრძალვა. ამიტომ ძალიან მნიშვნელოვანია მიახვედროთ, რომ არსებობს ზღვარი უწყინარ გართობასა და საშიშ, უადგილო რისკებს შორის.

- ესაუბრეთ მათ ინტერნეტ გამოწვევებზე. ჰკითხეთ, რას ფიქრობენ მათზე და თუ ჰქონიათ მათში მონაწილეობის მიღების სურვილი.

- შეახსენეთ, რომ ყველაფერი მათ ხელთაა და არ უნდა გააკეთონ ისეთი რამ, რაც არ მოსწონთ, იმ შემთხვევაშიც კი, თუ თანატოლები იწვევენ და მოუწოდებენ მათ ამა თუ იმ ქმედებისკენ.

- ურჩიეთ მათ გამოწვევაზე დათანხმებამდე დაფიქრდნენ ღირს თუ არა ამის გაკეთება.

- უთხარით ბავშვებს, რომ არ გაუგზავნონ გამოწვევები სხვებს, აუხსენით, რომ ამან დაუცველი ახალგაზრდები შეიძლება არაგონივრული რისკის ქვეშ დააყენოს.

ინტერნეტ დამოკიდებულება

აქვთ თუ არა თქვენს შვილებს ინტერნეტ დამოკიდებულება?

რადგან დღეს ციფრული ტექნოლოგიები ბავშვების ყოველდღიურობაში დიდ ადგილს იკავებენ, ადრინდელი ასაკიდანვე არსებობს ინტერნეტ დამოკიდებულების გაჩენის საშიშროება და ამას ზოგჯერ, მშობლებმაც შეიძლება შეუწყონ ხელი, როდესაც ბავშვებს გასართობად ტელეფონს ან პლანშეტს აძლევენ. ერთი შეხედვით უწყინარი თამაშები და მულტფილმების ყურება შესაძლოა ინტერნეტ დამოკიდებულებაში გადაიზარდოს.

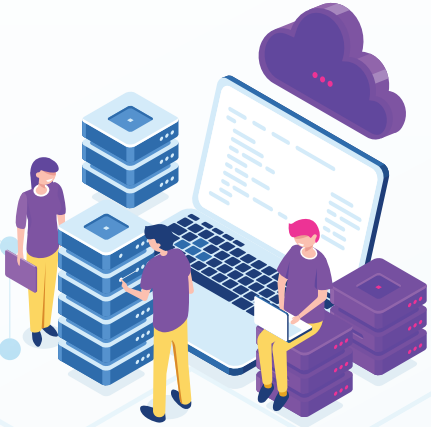
ინტერნეტ დამოკიდებულების შედეგები

ინტერნეტ დამოკიდებულებას მთელი რიგი უსიამოვნებების გამოწვევა შეუძლია, როგორიცაა მხედველობის დაზიანება, ხერხემლის, გულ-სისხლძარღვთა პრობლემები, სიმსუქნე, ნერვული სისტემის დაზიანება, ძილის დარღვევა, დეპრესია. ინტერნეტს ზოგჯერ ბავშვის ფსიქიკის დაზიანებაც შეუძლია. ამის მიზეზი შეიძლება იყოს ინტერნეტში არსებული უსაზღვრო თავისუფლება, სადაც აუარებელი გაუფილტრავი ინფორმაცია ინახება, ბავშვს არ შეუძლია მისი გადამუშავება, ამიტომ ის ყველაფერს იღებს და ამით ხშირად ფსიქიკას იზიანებს.

ინტერნეტ დამოკიდებულება

ბავშვები, რომლებსაც უჭირთ სოციალური ადაპტაცია, უფრო ხშირად ხდებიან ინტერნეტ დამოკიდებულები, რადგან ინტერნეტი მათ ანონიმურობის საშუალებას აძლევს. იმ შემთხვევაში, თუ რამეს არასწორად გააკეთებენ, ყოველთვის შეუძლიათ შეიცვალონ სახელი და ყველაფერი დაიწყონ თავიდან, ეს კი მოზარდს საფუძველს უქმნის კიდევ უფრო დაშორდეს რეალურს სამყაროს და მთლიანად გადაინაცვლოს ვირტუალურში, სადაც უფრო კომფორტულად გრძნობს თავს.

მეორეს მხრივ, ინტერნეტის დახმარებით, მორცხვი ბავშვი შეიძლება გახდეს უფრო კომუნიკაბელური, აქ მას შეუძლია იპოვნოს საკომუნიკაციო გარემო, რომელიც უფრო მეტად შეესაბამება მის განვითარების საფეხურს და, შედეგად, თვითშეფასებაც გაზარდოს. თუ თქვენი შვილი ჩაკეტილია საკუთარ თავში, მორცხვია ან იმედგაცრუებისკენ არის მიდრეკილი, ყურადღებით უნდა დააკვირდეთ მის აქტივობას ინტერნეტში, იმისათვის, რომ ციფრული ტექნოლოგიები, ბავშვის შესაძლებლობების გახსნის საშუალების ნაცვლად, უკონტროლო დამოკიდებულების ობიექტად არ იქცნენ.



ინტერნეტ დამოკიდებულება

ინტერნეტ დამოკიდებულების ნიშნების გამოვლენა

შეაფასეთ რამდენ დროს ატარებს თქვენი შვილი ინტერნეტში. კომპიუტერთან მუშაობის გამო, ხომ არ უგულებელყოფს საოჯახო საქმეს, საშინაო დავალების შესრულებას, ძილს, კვებას ან მეგობრებთან შეხვედრას.

ესაუბრეთ შვილს ინტერნეტში მისი აქტივობების შესახებ. სოციალური ქსელები სრული დაკავებულობის ილუზიას ქმნიან - რაც მეტ დროს ატარებს ბავშვი იქ, მით უფრო მეტი მეგობარი ჰყავს და მით უფრო მეტი მოცულობის ინფორმაციის დამუშავება ესაჭიროება.

დააკვირდით თქვენი შვილის ხასიათის ცვალებადობას და ქცევას ინტერნეტიდან გამოსვლის შემდეგ. შესაძლებელია დათრგუნულობის, გაღიზიანების, მოუსვენრობის, ურთიერთობისგან თავის არიდების სიმპტომების გაჩენა. ფიზიკური სიმპტომებიდან ხშირია თავის ან ზურგის ტკივილი, ძილის დარღვევა, ფიზიკური აქტივობის შემცირება, მადის დაკარგვა და სხვა.

ინტერნეტ დამოკიდებულება

ინტერნეტ დამოკიდებულების ნიშნების გამოვლენის შემთხვევაში:

- ეცადეთ ბავშვთან კონტაქტის დამყარება, გაიგეთ რა აინტერესებს ან აღელვებს მას.

- ინტერნეტის გამოყენების სრულად აკრძალვა არ იქნება შედეგის მომტანი, მაგრამ სასურველია მის გამოყენებაზე რეგლამენტის დაწესება. განსაზღვრეთ რამდენი დროის გატარება შეუძლია მას ინტერნეტში, აუკრძალეთ ქსელში შესვლა საშინაო დავალებების შესრულებამდე. მაგალითად ქსელში დროის შეზღუდვის მიზნით შეგიძლიათ მშობელთა კონტროლის სპეციალური პროგრამების გამოყენება.

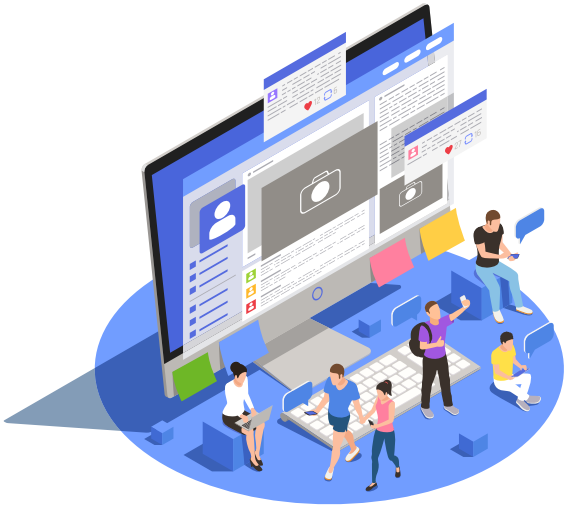
- სთხოვეთ ბავშვს, ერთი კვირის მანძილზე დეტალურად ჩაიწეროს, რაზე ხარჯავს დროს კომპიუტერთან მუშაობისას. ეს დაგეხმარებათ პრობლემის ნათლად დანახვაში, ასევე ზოგიერთი უსარგებლო ჩვევის მოშორებაში, მაგალითად: გვერდის მუდმივი განახლება ახალი შეტყობინებების მოლოდინში.

- შესთავაზეთ ბავშვს, რამეთი დაკავდეს თქვენთან ერთად, ეცადეთ მისი ვირტუალური საქმიანობა გადმოიტანოთ რეალურ ცხოვრებაში. მაგალითად ბევრ კომპიუტერულ თამაშს აქვს სამაგიდო ანალოგი, რომელშიც შეიძლება მთელი ოჯახის ან მეგობრების ჩართვა. აუცილებელია ბავშვს ჰქონდეს გასართობი, რომელიც არ უკავშირდება ინტერნეტს.

ინტერნეტ დამოკიდებულება

ინტერნეტ დამოკიდებულების მქონე ბავშვებს აქვთ ყალბი შეგრძნება, რომ ინტერნეტის გარეშე გაძლება შეუძლებელია. როგორც კი შესაძლებლობა მოგეცემათ, ბავშვთან ერთად განიხილეთ სიტუაცია, როდესაც ის რაიმე მიზეზით იძულებული გახდა ინტერნეტის გარეშე ყოფილიყო. მნიშვნელოვანია, ბავშვს ესმოდეს, რომ არაფერი მოხდება, თუ ის რაღაც დროით გამოეთიშება ონლაინ ცხოვრებას.

სერიოზული პრობლემების შემთხვევაში მიმართეთ სპეციალისტს, გაესაუბრეთ პედაგოგს ან ფსიქოლოგს. ინტერნეტის აკვიატებული გამოყენება სხვა პრობლემების სიმპტომი შეიძლება იყოს, როგორიცაა დეპრესია, გაღიზიანება და დაბალი თვითშეფასება და როდესაც ეს პრობლემები მოგვარდება, ინტერნეტ დამოკიდებულება შეიძლება თავისით გაქრეს.



დამნაშავეები ინტერნეტში

რა შეიძლება გააკეთოთ საფრთხის შესამცირებლად.

ინტერნეტის გამოყენებას კიდევ ერთი მნიშვნელოვანი საფრთხე ახლავს თან. ბავშვები შესაძლოა ბოროტმოქმედების პირისპირ მარტონი აღმოჩნდნენ. თქვენ შეძლებთ მოზარდის დაცვას იმ შემთხვევაში, თუ გეცოდინებათ ამ საფრთხეებისა და თქვენი შვილის ინტერნეტში საქმიანობის შესახებ.

ხომ არ იქცა თქვენი ბავშვი დამნაშავის პოტენციურ სამიზნედ?

ოჯახის კომპიუტერში გაჩნდა ეროტიული შინაარსის მასალები. გავრცელებულია მოზარდისათვის სექსუალური შინაარსის შემცველი ფოტო-ვიდეო მასალის გაგზავნა. ამ გზით ბოროტმოქმედი ცდილობს ბავშვი მოზარდსა და უფროსს შორის სექსუალური კავშირის ბუნებრივობაში დაარწმუნოს. გაითვალისწინეთ, რომ შესაძლოა მოზარდი მალავდეს ამ ფაილებს, განსაკუთრებით მაშინ, როცა ამავე კომპიუტერით ოჯახის სხვა წევრებიც სარგებლობენ.

თქვენს შვილს ურეკავენ თქვენთვის უცნობი პირები. ინტერნეტით კონტაქტის დამყარების შემდეგ, ბოროტმოქმედმა შესაძლოა სცადოს ბავშვის ინტიმურ ურთიერთობაში ჩათრევა ტელეფონით ან მასთან პირისპირ შეხვედრა. თუ მოზარდი ტელეფონის ნომრის მიცემისას ყოყმანობს, დამნაშავე მას თავად უზიარებს საკუთარ ნომერს.

ბავშვი ღებულობს წერილებს, საჩუქრებს ან გზავნილებს თქვენთვის უცნობი პირისგან. პირად შეხვედრაზე დათანხმების მიზნით, როგორც წესი, დამნაშავეები პოტენციურ მსხვერპლს უგზავნიან წერილებს, ფოტოებს და ზოგჯერ ძვირად ღირებულ საჩუქრებსაც კი.

დამნაშავეები ინტერნეტში

თქვენი ბავშვი თავს არიდებს ოჯახის წევრებს და მეგობრებს და თუ ოთახში ვინმე შედის დაუყოვნებლივ თიშავს მონიტორს ან გადადის სხვა ფანჯარაზე.

ინტერნეტ დამნაშავეები გულმოდგინედ ცდილობენ ბავშვსა და მშობლებს შორის ურთიერთობის გაფუჭებას და ხშირად აზვიადებენ ბავშვსა და ოჯახის წევრებს შორის მომხდარ უმნიშვნელო უსიამოვნებებს. გარდა ამისა სექსუალური დევნის ქვეშ მყოფი ბავშვი უფრო ჩაკეტილი და დათრგუნული ხდება.

თქვენი ბავშვი ინტერნეტში შესასვლელად სხვის პროფილს იყენებს. ბავშვი, რომელსაც სახლიდან არ აქვს ინტერნეტთან წვდომა, შეიძლება მაინც შეხვდეს დამნაშავეს, თუ გამოიყენებს ინტერნეტს მეგობრებთან ან სხვა საზოგადოებრივ ადგილებში. ზოგჯერ დამნაშავეები მსხვერპლს მზა პროფილით უზრუნველყოფენ.

როგორ მოვიქცეთ, თუ ბავშვი დამნაშავის სამიზნედ იქცა?

რეგულარულად შეამოწმეთ ხომ არ გაჩნდა თქვენი ოჯახის კომპიუტერში არასასურველი ფაილები. გააკონტროლეთ თქვენი შვილის საკომუნიკაციო საშუალებები, იქნება ეს მობილური ტელეფონი, პლანშეტი თუ პერსონალური კომპიუტერი. როგორც წესი, ინტერნეტ დამნაშავეები მსხვერპლს სოციალური ქსელების საშუალებით იცნობენ, შემდეგ კი მათთან ურთიერთობას პირად მიმოწერაში განაგრძობენ. არ დაადანაშაულოთ ბავშვი, თუ ინტერნეტით გაიცნობს კიბერ დამნაშავეს. მიიღეთ ყველა საჭირო ზომა ბავშვის ამ პირთან ურთიერთობის შეწყვეტის მიზნით. თუ თქვენი ბავშვი სექსუალური ხასიათის სურათებს იღებს ან სექსუალური შევიწროების მსხვერპლია, შეინახეთ ყველა არსებული მტკიცებულება, მიმოწერის და/ან მიმოწერისათვის გადაღებული ფოტოების ჩათვლით, იმისათვის, რომ შემდგომში ეს მასალები გადასცეთ სამართალდამცველებს.

არასანდო ინფორმაცია ინტერნეტში

დღეს ინტერნეტი უსაზღვრო შესაძლებლობებს იძლევა, მაგრამ ქსელში განთავსებული ინფორმაციის დიდი ნაწილი არ შეიძლება ჩაითვალოს სასარგებლოდ. ინტერნეტის მომხმარებლები კრიტიკულად უნდა აზროვნებდნენ, რათა მასალების სისწორის შეფასება შეძლონ, ვინაიდან უკლებლივ ყველას შეუძლია ინტერნეტში ინფორმაციის განთავსება.უპირველეს ყოვლისა, ეს ეხებათ ბავშვებს, რომლებიც ფიქრობენ, რომ ინტერნეტში განთავსებული ნებისმიერი ინფორმაცია შეესაბამება სიმართლეს. აუხსენით მოზარდს, რომ ინტერნეტს არ შეუძლია ქსელში განთავსებული ინფორმაციის სისწორის შემოწმება.

აუხსენით ბავშვს, როგორ მუშობს ინტერნეტი და, რომ ნებისმიერს შეუძლია საკუთარი ვებ-გვერდის გაკეთება და მასზე ნებისმიერი ინფორმაციის განთავსება. მან უნდა იცოდეს, რომელი წყაროების გამოყენება შეიძლება. ამასთან ერთად, მას უნდა შეეძლოს ქსელიდან მიღებული ინფორმაციის შემოწმება.

როგორ ვასწავლოთ ბავშვებს არასანდო, ფალსიფიცირებული მასალების გამოვლენა?

სწავლებების დაიწყება უმჯობესია პატარა ასაკიდანვე. დღეს, როცა უკვე სკოლამდელი ბავშვებიც იყენებენ ინტერნეტს, მნიშვნელოვანია მათ რაც შეიძლება ადრე ვასწავლოთ ფაქტების ვარაუდებისგან გარჩევა.

არასანდო ინფორმაცია ინტერნეტში

დაინტერესდით ბავშვის მიერ ინტერნეტში მოპოვებული ინფორმაციით.

ერთად განიხილეთ სხვადასხვა საიტები, შეამოწმეთ ამ საიტების რეალური დანიშნულება, არის თუ არა საიტზე განთავსებული საკონტაქტო ინფორმაცია ან განყოფილება „ჩვენ შესახებ“? საიტი ვინმეს მიერ ფინანსდება, თუ უბრალოდ საზოგადოებრივი დისკუსიების ადგილია?

დარწმუნდით, რომ ბავშვს შეუძლია დამატებით სხვა წყაროების გამოყენება ინფორმაციის სისწორის გადასამოწმებლად. მაგალითად, მასალების შესამოწმებლად, შეგიძლიათ მიმართოთ სხვა საიტებს ან საინფორმაციო რესურსებს - გაზეთებს, ჟურნალებსა და წიგნებს. მოზარდი წახალისებისთვის შეგიძლიათ წაიყვანოთ ბიბლიოთეკაში ან შეიძინოთ მათთვის ონლაინ ენციკლოპედია. ამგვარად ისინი ინფორმაციის ალტერნატიული წყაროების გამოყენებას მიეჩვევიან.

ძლიერი პაროლები

რაც უფრო მეტად ერთვებიან ბავშვები ონლაინ თამაშებში და სოციალურ ქსელებში, მით უფრო მნიშვნელოვანია, რომ მათ შეეძლოთ ძლიერი პაროლების შექმნა. კიბერ დამნაშავეებს უპრობლემოდ შეუძლიათ მარტივი პაროლების მქონე ანგარიშების გატეხვა.

როგორ ვასწავლოთ ბავშვებს პაროლების მართვა:

- აუხსენით ბავშვს, რომ ძლიერი პაროლების შექმნა ყველაფერზე მნიშვნელოვანია. რომ პაროლი უნდა შეიცავდეს მაღალი და დაბალი რეგისტრის ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს, პაროლს ასევე უნდა ჰქონდეს გარკვეული სიგრძე.

- აუხსენით ბავშვს პაროლის საჯარო კომპიუტერში შეყვანასთან დაკავშირებული საფრთხეები. საერთო გამოყენების კომპიუტერში შეიძლება იყოს რაიმე სახის მავნე პროგრამა, მათ შორის ისეთი, რომელსაც თქვენი პაროლის მოპარვა შეუძლია. ხოლო თუ ბავშვს ანგარიშიდან გამოსვლა დაავიწყდება, მასზე სრული კონტროლის მიღებას უცხო პირიც შეძლებს.

უსაფრთხოების და სიმარტივის თავსებადობა

მოუყევით ბავშვს, რომ ინტერნეტის ზოგიერთი მომხმარებელი ებმება კომფორტულობის ხაფანგში. ისინი საქმის გასამარტივებლად ერთ პაროლს იყენებენ რამდენიმე საიტისთვის და, რომ ეს კატეგორიულად მიუღებელია.

ძლიერი პაროლები

ორ ფაქტორიანი აუტენტიფიკაცია. ბავშვებმა ასევე უნდა იცოდნენ ორ ფაქტორიანი აუტენტიფიკაციის არსებობის შესახებ. ამ უსაფრთხოების მექანიზმის გამოყენებით მნიშვნელოვნად იზრდება ანგარიშის დაცვის დონე, ვინაიდან ის პროფილში შესვლისას დამატებით მოითხოვს დადასტურების კოდის შეყვანას. ორ ფაქტორიან აუტენთიფიკაციას შეუძლია შეზღუდოს დაშვება მონაცემთა გაჟონვის ან მოპარვის შემთხვევაში.

მოუყევით ბავშვებს, თუ რამდენად მნიშვნელოვანია პაროლების ხშირი განახლება.

როგორ ვასწავლოთ ბავშვს საიმედო პაროლის შექმნა.

არსებობს რამდენიმე მარტივი წესი, რომელიც ბავშვებმა უნდა დაიცვან:

- ბავშვმა მშობლების გარდა არავის არ უნდა გაუმხილოს თავისი სოციალური ქსელების და სათამაშო სერვერებზე არსებული ანგარიშების პაროლები, უახლოეს მეგობარსაც კი. აუხსენით ბავშვს, რომ პაროლის გამოტყუების შემდეგ კიბერ დამნაშავეს შეუძლია ღირებული სათამაშო ელემენტების მოპარვა ან მისი გვერდის გამოყენება ვირუსების და სპამის დასაგზავნად.

- არ შეიძლება პაროლების ფოსტით ან მესენჯერის ტიპის აპლიკაციებით გაგზავნა, როგორიცაა: Skype, Viber, WhatsApp და სხვა, იმ შემთხვევაშიც კი, თუ ამას სოციალური ქსელის ან სათამაშო სერვისის „თანამშრომელი“ მოითხოვს. დანამდვილებით შეიძლება ითქვას, სოციალური ქსელის ან სათამაშო სერვისის თანამშრომელი არასოდეს არ მოითხოვს პაროლს.

ძლიერი პაროლები

ასწავლეთ ბავშვს გრძელი და რთული პაროლების გამოყენება: მინიმალური სიგრძე - 12 სიმბოლო, დიდი და პატარა ასოების, ციფრების და სასვენი ნიშნების ჩათვლით. პაროლისთვის არ გამოიყენოს ისეთი ინფორმაცია რომელიც სხვებისთვისაცაა ცნობილი ან ციფრების მარტივი კომბინაცია, მაგალითად "12345". ნაცნობებიც ადვილად შეძლებენ მათ გამოცნობას, ხოლო, კიბერ დამნაშავეებს პაროლის გასატეხად შეუძლიათ სპეციალური პროგრამების გამოყენება. ერთი შეხედვით ბავშვს ეს შეიძლება რთულად მოეჩვენოს, მაგრამ სინამდვილეში არსებობს საიმედო პაროლის შექმნის მარტივი გზები.

ზოგიერთს საიმედო პაროლი წარმოუდგენია, როგორც შემთხვევითი ასოების და ციფრების კომბინაცია. ანუ, რაღაც ძალიან, ძალიან რთული დასამახსოვრებელი. მაგრამ თუ პრობლემას უსაფრთხოების პოზიციიდან მივუდგებით, აღმოჩნდება, რომ საკმაოდ რთული პაროლის დამახსოვრება არც თუ ისე ძნელი ყოფილა, რადგან არ არის აუცილებელი, რომ ის ციფრების და ასოების შემთხვევითი კომბინაციისგან შედგებოდეს.

როგორ უნდა მოვიფიქროთ ადვილად დასამახსოვრებელი და საიმედო პაროლი? პირველ რიგში, უნდა იყოს შერჩეული ბავშვისთვის მნიშვნელოვანი სიმბოლოების კომბინაცია, მისთვის მნიშვნელოვანი სიტყვის დამახსოვრება ბევრად უფრო ადვილი იქნება, ვიდრე სიმბოლოების შემთხვევითი ნაკრებისა, რომელსაც პროგრამა სთავაზობს.

ძლიერი პაროლები

ძლიერი პაროლის შედგენის მრავალი გზა არსებობს, მაგრამ უმჯობესია, პაროლები შეიქმნას ასოციაციების გამოყენებით.

საიმედო პაროლის მოსაფიქრებლად, რომელიც ბავშვს არასოდეს არ დაავიწყდება, შესთავაზეთ მას შემდეგი მოქმედებების შესრულება:

- შეარჩიეთ მოზარდის რომელიმე საყვარელი ფრაზა ან სტროფი სიმღერიდან, ფილმიდან ან მულტიპლიკაციური ფილმიდან, რომელიც ძალიან მოსწონს.
- ერთად ჩამოწერეთ პირველი ხუთი სიტყვის, პირველი ასოები.
- ყოველ ასოს შორის ჩაამატეთ ერთი სპეციალური სიმბოლო.

ამის შემდეგ მზად გექნებათ კომბინაცია, რომლითაც მიიღებთ უსაფრთხო პაროლს.

ერთადერთი, რაც დარჩა გასაკეთებელი, არის იმის გარკვევა, თუ როგორ უნდა გამოიყენოთ ასოციაციები, რომ ბავშვმა ადვილად დაიმახსოვროს თითოეული ვებ-გვერდისათვის განსხვავებული პაროლი.

ჰკითხეთ ბავშვს როგორი ასოციაციები უჩნდება, როდესაც ფიქრობს Facebook-ის, Instagram-ის და სხვა საიტების შესახებ, სადაც სურს დარეგისტრირება. გამოიყენეთ შექმნილი ასოციაციის პირველი ასო საბაზო კომბინაციის შესადგენად.

ძლიერი პაროლები

თუ ბავშვს სოციალური ქსელი აგონებს მეგობრების ცეკვას კამერის წინ, მაშინ შეგიძლიათ გამოიყენოთ სიტყვა «dance». ამგვარად, თუ ასოციაციურ ფრაზად აირჩევთ, მხიარულ სტრიქონს «Twinkle Twinkle Little Star How I Wonder What You Are», ხოლო სპეციალურ სიმბოლოდ, ინსტაგრამის მომხმარებელთა საყვარელ ნიშანს - «#», მაშინ პროფილის პაროლი იქნება «T#T#L#S#Hdance».

სიმბოლოების ეს კომბინაცია სხვა ნებისმიერი ადამიანისთვის უაზროა, მაგრამ რადგან თქვენმა ბავშვმა იცის სისტემა და საიტთან დაკავშირებული პირადი ასოციაციები, ეს პაროლი მისთვის ადვილი და გასაგები იქნება.

დაარიგეთ ბავშვი არ დაწეროს პაროლები ფურცლებზე და არ შეინახოს ისინი მყარ დისკზე. კიბერ დამნაშავე პირველ რიგში იქ დაიწყებს მათ ძებნას. პაროლის შენახვის საუკეთესო გზა, მისი დამახსოვრება ან პაროლების მენეჯერის გამოყენებაა (მაგ. LastPass სერვისი).

პაროლის შეყვანისას დარწმუნდეს, რომ ეს სწორედ ის საიტია, რომელიც სჭირდება.

კიბერ დამნაშავეები მომხმარებლების პაროლების მოპარვის მიზნით ხშირად აკეთებენ პოპულარული ვებ-გვერდების ასლებს. გვერდის სანდოობის გადამოწმების ყველაზე მარტივი გზა საიტის მისამართის ყურადღებით წაკითხვაა.

ძლიერი პაროლები

ძლიერი პაროლების გამოყენება აუცილებელია! მოსაზრება, რომ პაროლების დამახსოვრება ძნელია, არა მხოლოდ მცდარია, არამედ სახიფათოცაა!

ყოველთვის შეახსენეთ ბავშვს შემდეგი წესები:

- პაროლის სიგრძეს დიდი მნიშვნელობა აქვს.
- ყოველ საიტს უნდა ჰქონდეს საკუთარი უნიკალური პაროლი!
- საიმედო პაროლი - ეს არ არის აუცილებლად შემთხვევითი ნიშნების კომბინაცია, ეს რთულად გასატეხი სიმბოლოების თანმიმდევრობაა.
- პაროლები უნდა შეიქმნას ისეთ ფრაზებზე დაყრდნობით, რომლებიც ბავშვისთვის რაღაცას ნიშნავს და ის ადვილად დაიმახსოვრებს მათ!
- სხვისი კომპიუტერის გამოყენებისას უნდა გაითიშოს პაროლის დამახსოვრების ფუნქცია, წინააღმდეგ შემთხვევაში პაროლი შეინახება სხვის კომპიუტერში.

ბავშვების უსაფრთხოება ინტერნეტში

რის გაკეთება შეგიძლიათ ონლაინ სივრცეში თქვენი ბავშვების დასაცავად.

ბევრ მშობელს აწუხებს კითხვა, თუ როგორ უნდა უზრუნველყოს ბავშვების ინტერნეტ უსაფრთხოება? საბედნიეროდ, უკვე დიდი ხანია არსებობს ინტერნეტის უსაფრთხოების პროგრამული უზრუნველყოფა, რომლის დახმარებითაც ნებისმიერ მშობელს შეუძლია ბავშვების არასასურველი მასალის ან მავნე პროგრამების ჩამოტვირთვისგან დაცვა.

ბავშვების ინტერნეტზე წვდომის მართვა და მონიტორინგი.

ბავშვების ინტერნეტთან წვდომის მართვას გადამწყვეტი მნიშვნელობა აქვს და ამას ორი ფორმა გააჩნია:

მშობელთა კონტროლის პროგრამული უზრუნველყოფა თქვენი ბავშვის ინტერნეტში მუშაობის ყველა ასპექტის გაკონტროლების საშუალებას იძლევა, ონლაინ სივრცეში გატარებული დროის კონტროლის და გამოყენებული აპლიკაციებისა და ვებსაიტების ჩათვლით. აღნიშნული ინსტრუმენტის გამოყენებით შეძლებთ შეაჩეროთ დაბლოკილი პროგრამების ბავშვის მიერ გამოყენების მცდელობა და შეინახოთ იგი პროგრამის მეხსიერებაში, რომ თქვენთვის ყოველთვის ხელმისაწვდომი იყოს. დამატებითი პარამეტრების გამოყენებით შეგიძლიათ გარკვეულ კონტაქტებთან მიმოწერის, პირადი მონაცემების ან გარკვეული სიტყვებისა და ფრაზების შემცველი შეტყობინებების გაგზავნაც კი შეზღუდოთ.

ბავშვების უსაფრთხოება ინტერნეტში

ანტივირუსული პროგრამული უზრუნველყოფა დაგეხმარებათ ჯაშუშურ პროგრამებთან და ვირუსებთან გამკლავებაში, რომლებიც ძირითადად ინტერნეტიდან ხვდებიან კომპიუტერში. ანტივირუსული დაცვა მნიშვნელოვანია თქვენი ოჯახის ონლაინ უსაფრთხოებისთვის. ვებ-გვერდები, რომლებიც ლეგიტიმურად გამოიყურებიან, შეიძლება მავნე კოდს შეიცავდნენ. შექმენით ვირუსების ავტომატური შემოწმების გრაფიკი, ასევე ყოველთვიურად ჩაატარეთ სისტემის სრული სკანირება, იმისათვის, რომ თქვენს კომპიუტერში არ მოხვდნენ არასასურველი ან მავნე პროგრამები.

ნდობითა და პატივისცემით მოეპყარით მოზარდს

ბავშვებს უნდა ჰქონდეთ გარკვეული სივრცე იმისათვის, რომ ისწავლონ საკუთარი არჩევანის გაკეთება. ყველაფრის მკაცრი კონტროლი ვერ დაეხმარება მათ ამ ამოცანის განხორციელებაში, შეიძლება პირიქითაც მოხდეს და ისინი უფრო დაუმორჩილებლები გახდნენ.

საბოლოოდ მშობლებს ორ ფრონტზე უწევთ ბრძოლა:

1. ბავშვის მიერ ინტერნეტის შეუსაბამო გამოყენების შეზღუდვა.
2. მოზარდის მზარდი პირადი სივრცის პატივისცემა, რომელიც ასაკის მატებასთან ერთად გარდაუვალი ხდება.

პრაქტიკულად მშობლები ერთ შედეგამდე მიდიან - ინტერნეტის უსაფრთხოების მშობელთა კონტროლის საშუალებების გამოყენება უნდა ხდებოდეს ბავშვის პატივისცემის ფონზე. ბავშვის ინტერნეტ უსაფრთხოება იწყება მშობელთა კონტროლის საშუალებებით და მყარდება ანტივირუსული პროგრამებით. მაგრამ ეს არ უნდა ხდებოდეს ბავშვის თავისუფლების შეზღუდვის, მისი პირადი სივრცის შეზღუდვის ხარჯზე.

ბავშვების უსაფრთხოება ინტერნეტში

როგორ უნდა შეარჩიოთ დაცვის პროგრამული უზრუნველყოფა.

მშობელთა კონტროლის პროგრამული უზრუნველყოფის შეფასებისას მნიშვნელოვანია დარწმუნდეთ, რომ ის ინტერნეტ საფრთხეებისგან კომპლექსურ დაცვას უზრუნველყოფს.

ბავშვების ონლაინ უსაფრთხოება ნიშნავს:

- მათ დაცვას არასასურველი მასალებისგან.
- მათი მოწყობილობების მავნე პროგრამებისგან დაცვას.

მშობლის უსაფრთხოების გეგმა უნდა მოიცავდეს ყველა ზემოთ ჩამოთვლილ პარამეტრს. ინტერნეტ უსაფრთხოების უზრუნველყოფის საშუალებების უმეტესობა ინტერნეტიდან მომავალი საფრთხეებისგან სრულ დაცვას გვთავაზობს. ასეთი პროგრამების უამრავი ანალოგი არსებობს, ამიტომ არჩევანის გაკეთება შეიძლება რთული და მომაბეზრებელიც კი იყოს. საბედნიეროდ უფასო საცდელი ვერსიის გამოყენებით შეძლებთ გაეცნოთ პროგრამას და გაერკვეთ გამოდგება თუ არა ის თქვენი ოჯახისთვის.

რჩევები სხვადასხვა ასაკის ბავშვების ინტერნეტ უსაფრთხოებისთვის.

სტატისტიკის თანახმად 15-17 წლის მოზარდთა 80% აღიარებს, რომ ინტერნეტში არაერთხელ უნახავთ სექსუალური ძალადობის სცენები. 8-16 წლის ბავშვების 90% სასკოლო დავალებებისთვის დამატებითი ინფორმაციის ძებნის პარალელურად პორნოგრაფიულ ფილმებს უყურებდა. ამიტომ მშობლებმა შვილები უნდა აკონტროლონ და ასწავლონ როგორ გამოიყენონ ინტერნეტი უსაფრთხოდ.

ბავშვების უსაფრთხოება ინტერნეტში

რას აკეთებენ შვიდ წლამდე ასაკის ბავშვები ინტერნეტში?

ამ ასაკში ბავშვების ინტერნეტში საქმიანობა მშობლების აქტიური მონაწილეობით უნდა მიმდინარეობდეს. ამ ასაკის ბავშვები ადვილად ითვისებენ უახლეს ტექნოლოგიებს და გამოიმუშავებენ ინტერნეტის მოხმარებისათვის საჭირო ელემენტარულ ჩვევებს. მიუხედავად იმისა, რომ პატარები შეიძლება ძალიან ნიჭიერები იყვნენ თამაშებში და კომპიუტერში მოქმედებების შესრულებაში, ისინი სრულად არიან დამოკიდებულები უფროსებზე საიტების ძებნისას და ინტერნეტიდან მიღებული ინფორმაციის ინტერპრეტაციისას. უფროსები გადამწყვეტ როლს ასრულებენ ამ ასაკის ბავშვებისთვის ინტერნეტის უსაფრთხო გამოყენების სწავლების საკითხშიც. ამიტომ გამოიყენეთ ეს ასაკი რომ თქვენს შვილს ჩამოუყალიბოთ ინტერნეტში უსაფრთხოდ მუშაობის კულტურა.

რჩევები სკოლამდელი ასაკის ბავშვების უსაფრთხოების უზრუნველსაყოფად.

- ამ ასაკის ბავშვები ინტერნეტით უნდა სარგებლობდნენ მხოლოდ მშობლების ან სხვა უფროსების მეთვალყურეობის ქვეშ. განსაზღვრეთ ბავშვების ინტერნეტით და კომპიუტერით სარგებლობის დრო ექიმების და ფსიქოლოგების რეკომენდაციების მიხედვით.

- მოუყევით ბავშვებს კონფიდენციალურობის შესახებ. ასწავლეთ მათ არასოდეს გასცენ ინტერნეტით ინფორმაცია საკუთარი თავის და ოჯახის შესახებ. თუ რომელიმე საიტზე საჭირო გახდება ბავშვის სახელის შეყვანა, დაეხმარეთ მას ფსევდონიმის მოფიქრებაში, რომელიც არ გასცემს არანაირ პირად ინფორმაციას. მიაჩვიეთ ისინი, დროულად შეგატყობინონ თუკი ვინმე/რაიმე შეაწუხებთ ან დაემუქრებათ ინტერნეტში. შეინარჩუნეთ სიმშვიდე. შეახსენეთ მოზარდს, რომ საფრთხე აღარ ემუქრება, რადგან გაგენდოთ. ეს წაახალისებს ბავშვს, საჭიროების შემთხვევაში ისევ თქვენ მოგმართოთ.

ბავშვების უსაფრთხოება ინტერნეტში

რას აკეთებენ ინტერნეტში 7-დან 10 წლამდე ბავშვები?

ამ ასაკის ბავშვები აქტიურად იწყებენ ვირტუალური სივრცის დამოუკიდებლად გამოყენებას, უყვართ ინტერნეტში მოგზაურობა და ქსელური თამაშები, იყენებენ მესენჯერებს მეგობრებთან მიმოწერისთვის. თუმცა უნდა გაითვალისწინოთ, რომ ისინი შეიძლება ეწვიონ ვებ-გვერდებს რომელზე შესვლის უფლებაც თქვენ არ მიგიციათ. როგორც წესი ამ ასაკის ბავშვები ჯერ კიდევ არ ფლობენ კრიტიკული აზროვნების უნარებს, რაც აუცილებელია ინტერნეტში ნანახი მასალების ადეკვატური გააზრებისთვის.

უსაფრთხოების რჩევები 7-დან 10 წლამდე ასაკის ბავშვებისთვის.

- ინტერნეტში ჩართული კომპიუტერი დადგით საერთო სარგებლობის ოთახში, სადაც იოლად შეძლებთ თქვენი შვილის ინტერნეტ საქმიანობის გაკონტროლებას. ერთობლივად ჩამოაყალიბეთ ინტერნეტით სარგებლობის საშინაო წესები და მოითხოვეთ მათი შესრულება. მოითხოვეთ მათგან, რომ მხოლოდ იმ გვერდებს ეწვიონ, რომლის ნახვის უფლებაც თქვენ მიეცით. გამოიყენეთ არასასურველი მასალის ბლოკირების საშუალებები, ელექტრონული ფოსტის ფილტრები კონკრეტული პირების და განსაზღვრული სიტყვების და ფრაზების დასაბლოკად.

- იმის ნაცვლად, რომ ბავშვებს ჰქონდეთ საკუთარი ელექტრონული ფოსტის მისამართი, შექმენით ოჯახური ელექტრონული ფოსტის ყუთი, სადაც მოგივათ ყველა ელექტრონული შეტყობინება. ბავშვებმა თქვენთან უნდა გაიაროს კონსულტაცია ელექტრონული ფოსტით, ჩატში, განცხადებების დაფაზე და პირად ანგარიშში მიღებული წერილის გახსნამდე. ბავშვებმა თქვენი ნებართვის გარეშე არ უნდა ჩამოტვირთონ პროგრამები, ფაილები და მუსიკა.

ბავშვების უსაფრთხოება ინტერნეტში

ნება დართეთ მათ შევიდნენ მხოლოდ კარგი რეპუტაციის მქონე საბავშვო საიტებზე. ესაუბრეთ მათ ინტერნეტ მეგობრების და მათი საქმიანობის შესახებ, ისე როგორც რეალური მეგობრების შესახებ. მიაჩვიეთ ისინი შეგატყობინონ, თუ ვინმე ან რამე აწუხებთ ან ემუქრებათ.

რას აკეთებენ ინტერნეტში 10-დან 13 წლამდე ბავშვები?

ბავშვები ამ ასაკში იწყებენ ინტერნეტის გამოყენებას სასკოლო პროექტებზე სამუშაოდ. ამის გარდა ისინი ტვირთავენ მუსიკას, იყენებენ ელექტრონულ ფოსტას, აქტიურად თამაშობენ ონლაინ თამაშებს და შედიან თვიანთი საყვარელი მსახიობების ან მუსიკოსების ვებ გვერდებზე. უფრო მეტად იყენებენ შეტყობინებების მყისიერი გაცვლის საშუალებებს. ამ ასაკის ბავშვებს უჩნდებათ სურვილი გაარკვიონ, თუ რის გაკეთება შეუძლიათ მშობლების ნებართვის გარეშე. ამ დროს ბავშვმა შეიძლება სცადოს ისეთ საიტებზე და ფორუმებზე შესვლა, რის უფლებასაც თქვენ არ მისცემდით.

არ აუკრძალოთ ბავშვს ინტერნეტის გამოყენება, რადგან ის ნებისმიერ შემთხვევაში მოახერხებს ინტერნეტში შესვლას, და თქვენ არ გეცოდინებათ ამის შესახებ, რაც მეტ რისკს შეიცავს.

მშობელთა კონტროლის პროგრამული უზრუნველყოფის საშუალებების გამოყენების შემთხვევაში ბავშვებს არ გაუჩნდებათ შეგრძნება, რომ მშობლები მუდმივად ეკრანს უყურებენ. მაგრამ ამ სერვისის დახმარებით თქვენ გეცოდინებათ რომელ საიტებს სტუმრობს თქვენი შვილი.

ბავშვების უსაფრთხოება ინტერნეტში

რჩევები 10-დან 13 წლამდე ასაკის ბავშვების უსაფრთხოების უზრუნველსაყოფად.

- დარწმუნდით, რომ თქვენმა ბავშვმა იცის და იცავს ინტერნეტში ბავშვთა ქცევის წესებს. შეუქმენით ანგარიში შეზღუდული უფლებებით. მოზარდებთან ერთად შექმენით და დაიცავით ინტერნეტში მუშაობის საშინაო წესები. საჭიროა აკრძალული საიტების, ინტერნეტში ყოფნის საათების და ურთიერთობების დამყარების წესების განსაზღვრა. გამოიყენეთ არასასურველი მასალის გაფილტვრის საშუალებები.

- მოითხოვეთ ბავშვებისგან, რომ თქვენ გარეშე არასოდეს დასთანხმდნენ პირად შეხვედრებზე ინტერნეტ მეგობრებს. ასევე მოითხოვეთ მათგან არასოდეს გასცენ პირადი ინფორმაცია ონლაინ თამაშებში, ჩატებში, სარეგისტრაციო ფორმებში, პირად პროფილებში კონკურსებზე რეგისტრაციისას. გარდა ამისა აუხსენით, მათ, რომ ინტერნეტში ფოტო, ვიდეო მასალების ან სხვა ფაილების გადმოწერით ისინი შეიძლება არღვევდნენ საავტორო უფლებებს. მიაჩვიეთ ბავშვები, შეგატყობინონ, თუ რაიმე ან ვინმე დაემუქრება ან შეაწუხებს მათ ინტერნეტში. ზედამხედველობის განხორციელება უმჯობესია ბავშვების ღირსების, მათი პირადი სივრცის პატივისცემით.

- ბავშვებმა არავითარ შემთხვევაში არ უნდა გამოიყენონ ინტერნეტი ხულიგნობისთვის, ჭორების გასავრცელებლად, მუქარის და სხვა მსგავსი საქმიანობისთვის.

ბავშვების უსაფრთხოება ინტერნეტში

რას აკეთებენ ინტერნეტში 14-დან 17 წლამდე ბავშვები?

ამ ასაკის ბავშვებმა უკვე კარგად იციან, თუ რა სახის ინფორმაცია არსებობს ინტერნეტში. და სრულიად ნორმალურია ის ფაქტი, რომ მათ ამ ყველაფრის ნახვა, მოსმენა ან წაკითხვა უნდათ. არასასურველ მასალებზე წვდომა (მაგალითად პორნოგრაფიულ სურათებზე და ასაფეთქებლის გაკეთების ინსტრუქციებთან) შეიძლება ადვილად დაბლოკოთ პროგრამული ფილტრების დახმარებით. ამ ასაკში ისინი იწერენ მუსიკას, იყენებენ ელექტრონულ ფოსტას და სოციალურ ქსელებს, თამაშობენ და აქტიურად იყენებენ საძიებო საშუალებებს.

ბიჭები ამ ასაკში მიდრეკილნი არიან დაანგრიონ ყველა შეზღუდვა და ინტერესდებიან უხეში იუმორით, სისხლით, აზარტული თამაშებით და უფროსებისთვის განკუთვნილი სურათებით. გოგონებს უფრო მეტად მოსწონთ ჩატებში ურთიერთობა და ისინი ძალიან მოწყვლადები არიან ინტერნეტით სექსუალური შევიწროების მიმართ.

რჩევები 14-დან 17 წლამდე ასაკის ბავშვების უსაფრთხოების უზრუნველსაყოფად.

ამ ასაკის მოზარდებისთვის ინტერნეტში უსაფრთხოების უზრუნველყოფისთვის რჩევები იგივეა, რაც 13 წლამდე ასაკის ბავშვებისთვის, თუმცა აქ უკვე საჭიროა მეტი ყურადღება მიაქციოთ კონკრეტულ საკითხებს:

ბავშვების უსაფრთხოება ინტერნეტში

- მოზარდის მოთხოვნების შესაბამისად შეცვალეთ ინტერნეტის მოხმარების საშინაო წესები, მოითხოვეთ მათი შესრულება. ისაუბრეთ მოზარდებთან თავიანთ ინტერნეტ მეგობრების და მათი საქმიანობის შესახებ, სასურველია რომ უკეთ გაიცნოთ ისინი.

- მეტი ყურადღება მიაქციეთ მოზარდებში პოპულარულ ინტერნეტ ტენდენციებისა და სხვადასხვა გამოწვევებს. ასეთი ტიპის აქტივობები ხშირად ორიენტირებულია მოზარდის მოტყუებაზე და წარმოდგენილია თამაშის ან საინტერესო აქტივობის სახით. თუკი შეამჩნევთ, რომ მოზარდი ამ თემებით ინტერესდება, ამ საკითხში უკეთ უნდა გარკვეთ, რათა მოზარდს დაანახოთ მათგან მომვალი საფრთხეები.

- თუ შეამჩნიეთ რომ მოზარდი ინტერესდება ინტერნეტში აზარტული თამაშებით, საჭიროა გაარკვიოთ რამ გამოიწვია მისი ამ საკითხით დაინტერესება: რეკლამაში წარმოდგენილმა გრანდიოზული პრიზის მოგების შესაძლებლობამ თუ თანატოლების მიერ მიწოდებულმა ინფორმაციამ. ამ შემთხვევაში საჭიროა მოზარდთან მეტი საუბარი და იმის ჩვენება თუ რამხელა ზიანის მიყენება შეუძლია მოზარდის ფსიქიკისთვის და მისი ოჯახისთვის ამ მავნე ჩვევას.

- ურჩიეთ გაიარონ კონსულტაცია ინტერნეტით ნებისმიერი ნივთის ყიდვის ან გაყიდვის დროს.

ბავშვების უსაფრთხოება ინტერნეტში

- თუ თქვენი შვილი თქვენზე უკეთ ერკვევა პროგრამულ უზრუნველყოფაში, გადააბარეთ მას საოჯახო კომპიუტერის უსაფრთხოების საკითხები.
- შეამოწმეთ თქვენი საბანკო ბარათისა და ტელეფონის გადახდები უცნობ ანგარიშზე.
- გაარკვიეთ, თუ არსებობს, ონლაინ დაცვა თქვენი ბავშვის სკოლაში, სკოლის შემდგომი ცენტრის, მეგობრების სახლებში ან ნებისმიერ ადგილას, სადაც ბავშვს თქვენი მეთვალყურეობის გარეშე შეუძლიათ კომპიუტერის გამოყენება.
- მიუდექით თქვენს შვილს სერიოზულად, თუ ის გაცნობებთ არასასიამოვნო ონლაინ მიმოწერის შესახებ.
- ესაუბრეთ თქვენს შვილებს! შეინარჩუნეთ კომუნიკაციის ღია ხაზი და დარწმუნდით, რომ ისინი კომფორტულად გრძნობენ თავს, როდესაც თქვენ მოგმართავენ თუ ინტერნეტით პრობლემები ექმნებათ.

ტექნოლოგიები განათლებაში

ინტერნეტი მნიშვნელოვან როლს ასრულებს განათლებაში. თანამედროვე ეპოქაში ტექნოლოგიების მომხმარებლები კითხვებზე პასუხების პოვნისთვის ინტერნეტში საძიებო სისტემებს მიმართავენ. საძიებო სისტემების მაგალითებია Google, Yahoo და სხვა. ასეთი მიდგომა მომხმარებელს სულ რაღაც წამებში აძლევს სასურველი ინფორმაციის მიღების საშუალებას. ინტერნეტი შეიცავს უსაზღვრო ინფორმაციას, რომლის ძებნა ნებისმიერ დროს არის შესაძლებელი. ინტერნეტმა ახალ სიმაღლეზე აიყვანა ტექნოლოგიების, კომუნიკაციისა და ონლაინ გართობის საშუალებები.

ინტერნეტი მოსწავლეებს უმარტივებს სასკოლო კვლევების შესრულებას და სკოლაში გავლილი მასალის გამეორებას. მოსწავლეები მას იყენებენ საკუთარი საჭიროების და ინტერესების შესაბამისად.

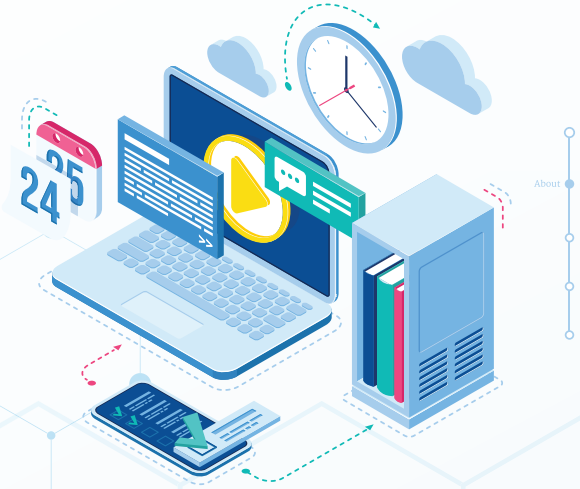
ინტერნეტის უპირატესობები განათლების სფეროში:

- ხელმისაწვდომი განათლება. განათლების მიღების ერთ-ერთი უდიდესი ბარიერი არის მისი მაღალი ღირებულება. ინტერნეტი აუმჯობესებს განათლების ხარისხს, რაც არის ქვეყნის მდგრადი განვითარების ერთ – ერთი საყრდენი. უზრუნველყოფს განათლებას ვიდეოების საშუალებით (მაგ. YouTube-ის სასწავლო ვიდეოები) და ვებ – სახელმძღვანელოებით, რომლებიც ყველასთვის ხელმისაწვდომი და ეფექტურია.

ტექნოლოგიები განათლებაში

მოსწავლე - მასწავლებლის და თანატოლების ურთიერთთანამშრომლობა. ინტერნეტი მოსწავლეებს საშუალებას აძლევს მუდმივი კონტაქტი ჰქონდეთ მასწავლებლებთან ან თანაკლასელებთან, სოციალური ქსელების, შეტყობინებების გაგზავნისა და ჩატის ფორუმების დახმარებით. თანამოაზრეებთან ურთიერთობა ფორუმზე შეიძლება დაეხმაროს მოსწავლეებს ახალი იდეების კვლევაში და ცოდნის გამდიდრებაში. მშობლებს ასევე შეუძლიათ ურთიერთობა მასწავლებლებთან და სკოლის ადმინისტრაციასთან.

სწავლებისა და სწავლის ეფექტური ინსტრუმენტი. ინტერნეტი გახდა როგორც ეფექტური სწავლების, ასევე სწავლის მთავარი ინსტრუმენტი. მასწავლებლებს შეუძლიათ ის გამოიყენონ როგორც სასწავლო სახელმძღვანელო, ატვირთავენ რა სასწავლო მასალებს შენიშვნებსა და ვიდეოებს სკოლის ვებსაიტზე ან ფორუმზე. სასწავლო პროცესი საინტერესო და მრავალფეროვანი ხდება სასწავლო ვიდეოების გამოყენებით. მასწავლებლებს შეუძლიათ ანიმაციის, PowerPoint-ის სლაიდების და სურათების გამოყენება მოსწავლეთა ყურადღების მისაპყრობად.



ტექნოლოგიები განათლებაში

ხარისხიანი განათლებაზე წვდომა. ბავშვებს მარტივად შეეძლებათ მიიღონ ხარისხიანი სასწავლო მასალები, როგორიცაა სასწავლო ვიდეოები YouTube-ზე (უფასოდ) ან გადაიხადონ საფასური ინტერნეტით, უფრო ხარისხიანი სასწავლო მასალებისთვის. მასწავლებლებს ასევე შეუძლიათ ისარგებლონ ინტერნეტით და სტუდენტები უზრუნველყონ დამატებითი სასწავლო რესურსებით, როგორიცაა ინტერაქტიული გაკვეთილები, საგანმანათლებლო ვიქტორინა და სახელმძღვანელოები. მასწავლებლებს შეუძლიათ ჩაიწერონ თავიანთი ლექციები და მიაწოდონ სტუდენტებს განსახილველად.

სოციალურ ქსელებთან ურთიერთობა. სოციალური ქსელების რეგულარული გამოყენება ჩვენი ცხოვრების ერთ – ერთი ძირითადი ნაწილია. განცხადებების ციფრული დაფები ზოგავს ქაღალდს, სტუდენტების ყურადღების კონცენტრაციისთვის იძლევა ვიდეორგოლების და აუდიო ჩანაწერების ჩვენების საშუალებას. დღეისათვის არსებობს მრავალი ფასიანი საიტი, რომელიც უზრუნველყოფს მაღალი ხარისხის საგანმანათლებლო მასალებს, რომლებიც ადვილად გასაგებია მასებისთვის.

ინფორმაციის მუდმივი განახლება. ინფორმაცია ყველაზე დიდი უპირატესობაა, ინტერნეტში შეგვიძლია ინფორმაციის მოძიება ყველა ჩვენთვის საინტერესო საკითხზე.

სწავლა მულტიმედიის დახმარებით. ეს ეხმარება ბავშვებს სასწავლო პროცესში, რადგან ეს ცოდნის მიღების პროცესს ამარტივებს. ასევე ხელს უწყობს ვიზუალიზაციას, თუ რას ასწავლიან მასწავლებლები სკოლაში.

კიბერუსაფრთხოება საქართველოში

საქართველოს კიბერუსაფრთხოების კანონმდებლობის მიმოხილვა.

2008 წელს კიბერ-შეტევამ საქართველოს წინააღმდეგ აშკარად აჩვენა საქართველოს კიბერუსაფრთხოების პოლიტიკის ნაკლოვანებები. არ არსებობდა შესაბამისი კანონმდებლობა და არც სტრატეგია, რომელიც უზრუნველყოფდა ქვეყნის თავდაცვისუნარიანობას ახალი კიბერ გამოწვევების წინააღმდეგ.

2010 წელს, მთავრობამ მიიღო „საქართველოს საფრთხეების შეფასების დოკუმენტი 2010–2013“, რომელშიც კიბერსივრცის დაცვა აღიარებულ იქნა ქვეყნის ეროვნული უსაფრთხოების ერთ-ერთ მთავარ საკითხად. 2010 წელს, საქართველოს სისხლის სამართლის კოდექსს დაემატა კიბერდანაშაულისა და კიბერუსაფრთხოების თავი, რის შემდეგაც სახელმწიფომ დამატებით შეიმუშავა დოკუმენტი კიბერუსაფრთხოების შესაძლებლობების გაუმჯობესების შესახებ. 2012 წელს ევროპული საბჭოს კიბერუსაფრთხოების კონვენციის რატიფიცირების შემდეგ, საქართველო ოფიციალურად შეუერთდა იმ ქვეყნების სიას, რომლებმაც გამოუცხადეს ომი კიბერდანაშაულს.

ერთის მხრივ, ეფექტური კიბერუსაფრთხოების გარემოს შესაქმნელად, სახელმწიფოს სჭირდებოდა შესაბამისი კანონმდებლობა, რომლის ფარგლებშიც იქნებოდა მიღებული ახალი სამოქმედო გეგმები და სტრატეგიები, ხოლო, მეორეს მხრივ, კიბერუსაფრთხოების სამოქმედო გეგმების საფუძველზე, მთავრობას შეეძლო სახელმწიფო კიბერუსაფრთხოების შენარჩუნებაზე პასუხისმგებელი უწყებების შექმნა.

კიბერუსაფრთხოება საქართველოში

2012 წლის 5 ივნისს საქართველოს პრეზიდენტმა ხელი მოაწერა კანონს ” ინფორმაციის უსაფრთხოების შესახებ”.

კანონი 4 თავისა და 12 მუხლისგან შედგება, რომლებიც განსაზღვრავს სახელმწიფოს კიბერ უსაფრთხოების პოლიტიკის საკითხებს:

თავი I - „ზოგადი დებულებები“ (მუხლი 1 - „კანონის მიზანი“; მუხლი 2 - „ტერმინების განმარტება“; მუხლი 3 - „კანონის მოქმედების სფერო“);

თავი II - ”ინფორმაციის უსაფრთხოების ორგანიზება და უზრუნველყოფა” (მუხლი 4 - ინფორმაციის უსაფრთხოების წესები; მუხლი 5 - ინფორმაციის აქტივების მენეჯმენტი; მუხლი 6 - ინფორმაციის უსაფრთხოების შეფასება და ინფორმაციული სისტემების ტესტირება; მუხლი 7 - ინფორმაციის უსაფრთხოების მენეჯერი);

თავი III - ინტერნეტუსაფრთხოების უზრუნველყოფა + თავი III-1 - კიბერუსაფრთხოების ბიურო (მუხლი 8 - მონაცემთა გაცვლის სააგენტოს გადაუდებელი კომპიუტერული რეაგირების ჯგუფი; მუხლი 9 - კიბერუსაფრთხოების სპეციალისტი; მუხლი 10 - კომპიუტერული ინციდენტების იდენტიფიკაცია; მუხლი 10.1 - კიბერუსაფრთხოების ბიუროს სტატუსი და ფუნქციები მუხლი 10.2 - კიბერუსაფრთხოების ბიუროს დირექტორი; 10.3 მუხლი - კიბერუსაფრთხოების ბიუროს CERT);

კიბერუსაფრთხოება საქართველოში

თავი IV - გარდამავალი და დასკვნითი დებულებები (მუხლი 11 - გარდამავალი დებულებები; მუხლი 12 - საბოლოო დებულება).

ამ კანონით შეიქმნა იურიდიული საფუძველი სახელმწიფო კიბერუსაფრთხოებისგანვითარებისათვის. გამოიკვეთაამპროცესზეპასუხისმგებელი სახელმწიფო ორგანოები და კიბერუსაფრთხოების სამოქმედო გეგმის შემუშავება საქართველოს პოლიტიკური დღის წესრიგის ნაწილი გახდა.

2013 წლის 11 მარტს, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად, პრეზიდენტმა დაამტკიცა კრიტიკული ინფორმაციული სისტემის საგნების ჩამონათვალი. საერთო ჯამში, შეირჩა 36 ობიექტი და მონაცემთა გაცვლის სააგენტო CERT აიღო პასუხისმგებელობა ამ სუბიექტებისთვის კიბერუსაფრთხოების სერვისების მიწოდებაზე. 2014 წლის 29 აპრილს საქართველოს მთავრობამ არსებულ სიაში დაამატა 3 ობიექტი.

ლექსიკონი

პროფილი (ინგლ. Account) - პროფილი, სარეგისტრაციო ანგარიში.

ანტივირუსი - კომპიუტერული პროგრამების პაკეტი, რომელიც აკავებს ვირუსებს და არ უშვებს მათ შენს კომპიუტერში. ამოწმებს არის, თუ არა კომპიუტერში ჩაწერილ ფაილებში ვირუსი. ანტივირუსი ასევე ახდენს ფაილების დეზინფექციას და წაშლას.

ბრაუზერი - პროგრამა, რომელიც ინტერნეტში ვებ-გვერდებზე შესვლის საშუალებას გვაძლევს. ყველაზე პოპულარული ბრაუზერებია Opera, Mozilla Firefox, Google Chrome, Internet Explorer.

ვირუსები - მავნე პროგრამები, რომლებიც ხელს უშლიან კომპიუტერის ნორმალურ მუშაობას, გადაწერენ, აზიანებენ ან შლიან მონაცემებს.

ინტერნეტი (ინგლ. Internet) - „მსოფლიო-ქსელი“, ერთმანეთზე მიერთებული კომპიუტერების საჯაროდ ხელმისაწვდომი ქსელი. ინტერნეტი აღნიშნავს გლობალურ კომპიუტერულ ქსელს.

ბულინგი (ჩაგვრა) - ბულინგი გულისხმობს თანატოლთა შორის ჩაგვრას, რომელიც დროთა განმავლობაში მეორდება და მიზნად ისახავს ადამიანისთვის ფიზიკური ან/და ემოციური ზიანის მიყენებას. იგი მოქმედებს ადამიანის ემოციურ მდგომარეობაზე და ლახავს მის რეპუტაციას. ბულინგი შეიძლება იყოს ფიზიკური, ვერბალური, სოციალური და კიბერბულინგი.

ინტერნეტ დამოკიდებულება - ინტერნეტის გადაჭარბებული გამოყენება, ქსელში დროის გადაჭარბებული ხარჯვა.

სპამი - წერილების გაგზავნა მიმღების თანხმობის გარეშე.

ლექსიკონი

კიბერბულინგი - ბულინგის სახეობა, რომელიც ონლაინ სივრცეში ხორციელდება შეურაცხყოფის შემცველი შეტყობინებებით, აგრესიით, დაშინებით, სხვადასხვა ინტერნეტსერვისების საშუალებით.

ონლაინ თამაშები - თამაშის პროცესი, რომელიც ეფუძნება სხვა მოთამაშეებსა და სათამაშო სამყაროს ურთიერთქმედებას, მოითხოვს ინტერნეტთან მუდმივ კავშირს.

პაროლი - უსაფრთხოების საშუალება, სიმბოლოების ნაკრები, რომელიც ცნობილია მხოლოდ ერთი მომხმარებლისთვის, საჭიროა ვებგვერდზე შესასვლელად.

სოციალური ქსელები - ინტერნეტში განთავსებული საიტები, მსგავსი ინტერესების მქონე ადამიანების თავშეყრის ადგილი ონლაინში. ასეთი საიტები გამოიყენება კომუნიკაციისთვის, შეხვედრისთვის და ადამიანებთან ურთიერთობის დასამყარებლად.

„ტროას ცხენი“ - მავნე პროგრამა რომლის მეშვეობითაც ხდება მომხმარებლის კომპიუტერულ მონაცემებზე წვდომა. ტროიანებმა შეიძლება შეაღწიონ კომპიუტერში ინტერნეტ აპლიკაციების მეშვეობით. ტროიანი ავტომატურად ინსტალირდება ჩამოტვირთულ აპლიკაციასთან ერთად კომპიუტერზე კონტროლის მისაღებად.

ფიშინგ შეტყობინებები - მოტყუების გზით ცდილობენ მიიღონ მნიშვნელოვანი ინფორმაცია, ისეთი როგორიცაა პაროლები ან სხვა პირადი მონაცემები.

მავნე პროგრამა - პროგრამა, რომელიც ხელს უშლის კომპიუტერის ნორმალურ მუშაობას. ხშირ შემთხვევაში მავნე პროგრამა შეიძლება გამოყენებული იყოს მსხვერპლის კომპიუტერიდან ინფორმაციის მოსაპარად.

ჩატი - ინტერნეტის გამოყენებით რეალურ დროში პირადი შეტყობინებების გაცვლის საშუალება.