ინტერნეტში უსაფრთხოების გზამკლევი ბავშვებისთვის

ასაკი: 6-11 წელი

World Vision

მაქსიმ იავიჩი
გიორგი იაშვილი

2020

სარჩევი

რა არის ინტერნეტი 1
ვინ ხარ ინტერნეტში 2
სოციალური ქსელები 4
სოციალური ქსელები და უცნობები 5
რისთვის გვჭირდება პაროლი 6
დამნაშავეები ინტერნეტში 7
ონლაინ ბულინგი 8
რა არის მავნე პროგრამები და ვირუსები 9
თამაშზე დამოკიდებულება 11
ინტერნეტში ქცევის წესები 12
არ გასცე პირადი ინფორმაცია 14
სოციალურ ქსელებში ქცევის წესები 15
უსაფრთხოების წესები ინტერნეტში 17
პაროლები და უსაფრთხოება 18
ლექსიკონი 24

რა არის ინტერნეტი

ინტერნეტი არის ერთმანეთზე მიერთებული კომპიუტერების საჯაროდ ხელმისაწვდომი ქსელი, სადაც მომხმარებლებს, შეუძლიათ ნებისმიერი კომპიუტერიდან მიიღონ ინფორმაცია.

რაში ვიყენებთ ინტერნეტს

ინტერნეტი გაძლევს სამყაროს, ბუნების, სხვადასხვა ხალხისა და კულტურის წესების, სახლიდან გაცნობის უნიკალურ შესაძლებლობას. აუცილებელი არ არის ათასობით კილომეტრის გავლა იმისათვის, რომ საინტერესო ვირტუალური ექსკურსია მოიწყო ყველაზე უცნაურ კუნძულზე. ინტერნეტის საშუალებით, ასევე შეგიძლია უფრო ახლოს გაეცნო სახიფათო გარეულ ცხოველებს.

ინტერნეტ ტექნოლოგიების საშუალებით შეგიძლია ისწავლო მსოფლიოს ნებისმიერი ენა, ხატვა და ჟონგლირებაც კი.

წიგნების კითხვა, მუსიკის მოსმენა, მულტფილმების და ფილმების ყურება - ინტერნეტი შლის შენს წინაშე ახალ სამყაროს და ყოველდღე გჩუქნის ახალ აღმოჩენებს.

მესენჯერების საშუალებით შეგიძლია კავშირი იქონიო ახლობლებთან, თუნდაც ისინი პლანეტის მეორე მხარეს იმყოფებოდნენ.

ინტერნეტში შეგიძლია საგანმანათლებლო თამაშების თამაში სადაც მუდმივად კონცენტრირებული უნდა იყო და თვალყური ადევნო კომპიუტერის მონიტორზე ან ტაბლეტზე მიმდინარე ცვლილებებს. ეს ხელს უწყობს ფოკუსირების და აზროვნების განვითარებას.

ვინ ხარ ინტერნეტში

ვინ ხარ შენ? შენი საუკეთესო მეგობრები შეიძლება ფიქრობენ, რომ შენ მხიარული, სერიოზული, გართობის ან კიდევ ზედმეტი ლაპარაკის მოყვარული ხარ. შენმა მასწავლებლებმა კი, შეიძლება იფიქრონ, რომ შენ კრეატიული მოსწავლე, ნიჭიერი მსახიობი, სპორტსმენი, შრომისმოყვარე ადამიანი ან სულაც ხუმარა ხარ.

ჩვენი საუბრის თემა შენი ვინაობაა - ვინ ხარ, რას ფიქრობ საკუთარ თავზე, რას ფიქრობენ სხვები შენზე?

რა თქმა უნდა, შენ ყოველთვის შენ ხარ, მაგრამ ალბათ სხვადასხვა ვინაობებიც გექნება, იმის მიხედვით, თუ რა სიტუაციაში ან ვისთან ერთად იმყოფები. მაგალითად, სკოლაში შეიძლება მშვიდი იყო, ხოლო სახლში შესაძლოა გიცნობდნენ, როგორც პირწავარდნილ ხუმარას.

ისევე როგორც რეალობაში, ინტერნეტშიც გაქვს ონლაინ ვინაობა, რომელიც შეგიძლია შექმნა იმის მიხედვით, თუ რისთვის იყენებ ინტერნეტს - სწავლისთვის, თამაშისთვის, გართობისთვის, მეგობრებთან ურთიერთობისთვის თუ სხვა.

ვინ ხარ ინტერნეტში

აპლიკაციები და ვებგვერდები მომხმარებლის სახელის არჩევის საშუალებას გაძლევენ. თუ გინდა, რომ გიცნობდნენ, როგორც “King_of_Ketchup” (კეტჩუპის მეფე) - ეს შენი ახალი სახელი იქნება. მაგრამ, თუ შენ საკუთარ თავს კეტჩუპის მეფეს უწოდებ, ნიშნავს ეს, რომ შენ მართლა გიყვარს კეტჩუპი? მოუყვები შენს ახალ ონლაინ მეგობრებს, თუ, როგორ გიყვარს კეტჩუპი? ეს შენზეა დამოკიდებული, მაგრამ ეს აჩენს საინტერესო კითხვას: რამდენად ბევრი უნდა გააზიარო შენი რეალური პიროვნების შესახებ ინტერნეტში?

შესაძლოა თავი მშვენივრად იგრძნო, როდესაც მეგობრებს შენი უდიდესი გატაცების შესახებ უყვები, მაგრამ რა მოხდება, თუ მთელი სკოლა ნახავს შენს ლექსს, რომელიც შეყვარებულის ლამაზ თვალებს მიუძღვენი? რა მოხდება, თუ უცნობები ნახავენ მას?

არსებობს ინტერნეტში ქცევის წესები, ზუსტად ისევე, როგორც რეალურ ცხოვრებაში. მათი ცოდნა მნიშვნელოვანია იმისათვის, რომ შეძლო ინტერნეტში უსაფრთხოდ სწავლა და გართობა.

სოციალური ქსელები

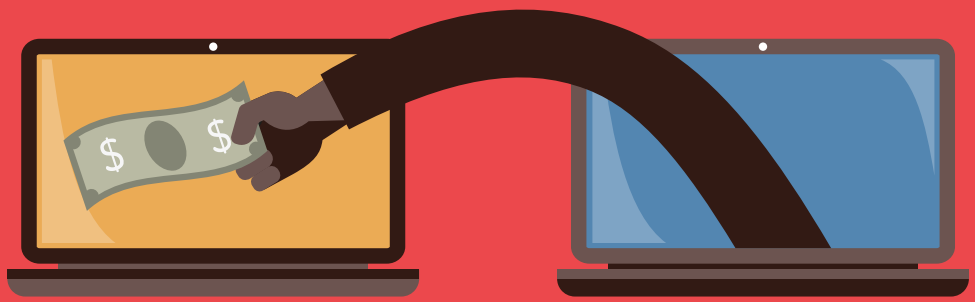
Facebook, Instagram და სხვა მსგავსი საიტები მეგობრებთან ინტერნეტით ურთიერთობის საშუალებას გაძლევენ, ამიტომ მათ სოციალურ ქსელებს უწოდებენ.

სოციალური ქსელების საშუალებით ასევე შეგიძლია ურთიერთობის დამყარება, ფოტოების გაზიარება, მეგობრებთან თამაში, საკუთარი თავის შესახებ სხვებისთვის მოყოლა და საინტერესო ინფორმაციის მიღებაც კი. თუ ერთ-ერთ ასეთ გვერდზე პროფილის შექმნას გადაწყვეტ, უმჯობესი იქნება ჯერ დედას ან მამას დაელაპარაკო ამის შესახებ.

სოციალური ქსელები და უცნობები

თუ Minecraft-ის ან Clash of Clans -ის მოყვარული ხარ, გეცოდინება, რომ შეგიძლია ეწვიო სხვა მოთამაშეების მიწებს და ესაუბრო მათ ონლაინში. ბავშვებმა, რომლებიც Wii-ით, Xbox-ით ან საკუთარი კომპიუტერით, ტაბლეტით, სმარტფონით ან სხვა მოწყობილობებით თამაშობენ, ისწავლეს, თუ როგორ დაამყარონ ურთიერთობები სათამაშო ვებ-გვერდებზე, ნაცნობებთან და უცნობებთანაც კი.

ბავშვები ხშირად ტყუვდებიან იმათ მიერ, ვინც თავს კარგ ადამიანად ასაღებს. მეორე მხარეს მყოფმა პირმა შეიძლება ძალიან სასიამოვნო ადამიანად მოგაჩვენოს თავი, მან შეიძლება გითხრას, რომ ჭკვიანი და საყვარელი ხარ. ვიღაც შეიძლება გწერდეს, რომ ისიც შენსავით მეექვსე კლასშია, სინამდვილეში კი ზრდასრული ადამიანი იყოს. ზოგიერთი ბავშვი სახიფათო მდგომარეობაში აღმოჩნდა, როდესაც დათანხმდა პირადად შეხვედროდა საიდუმლოებით მოცულ ონლაინ მეგობარს ან გაანდო სახლის ან სკოლის მისამართი და სხვა პირადი ინფორმაცია.



რისთვის გვჭირდება პაროლი

იმისათვის, რომ შეხვიდე ონლაინ თამაშში ან სოციალურ ქსელში გჭირდება მომხმარებლის სახელი და პაროლი.

პაროლი შეიძლება სახლის გასაღებს შევადაროთ. ყველა ბავშვმა იცის, რომ არ შეიძლება უცნობისთვის გასაღების მიცემა, ვინაიდან ის ნებართვის გარეშე შეძლებს თქვენს სახლში შემოსვლას. ასევე პაროლი შეიძლება შევადაროთ კბილის ჯაგრისს, ის უნდა შეიცვალოს ყოველ 3-4 თვეში, რადგან ის ძველდება და კარგავს ეფექტურობას.

დამნაშავეები ინტერნეტში

ჰაკერები და კიბერ დამნაშავეები მხოლოდ ფილმებში არ გვხვდება. რეალურად ინტერნეტში უამრავი უცნაური პირი და ბოროტმოქმედია. ისინი ათასგვარ ხრიკს მიმართავენ სმარტფონების ვირუსით დასაზიანებლად, სხვისი Facebook-ის ან Instagram-ის გასატეხად ან World of Tanks-ში ყველაზე მაგარი ტანკის მოსაპარად.

მათთვის საერთოდ არ აქვს მნიშვნელობა, ვის გაძარცვავენ - შენ თუ შენს მეგობარს. ამიტომ, ქსელში შესვლისას საჭიროა ბოროტმოქმედებზე უფრო ჭკვიანი იყო.

ონლაინ ბულინგი

როდესაც კომპიუტერს იყენებ, შეიძლება მაცდუნებლად მოგეჩვენოს მომხმარებლის სახელის მიღმა დამალვის იდეა, იმისათვის, რომ ვიღაცას გაეხუმრო, ან გააბრაზო, ან კიდევ სხვა ვინმედ მოაჩვენო თავი. ან იქნებ ვინმეზე გაბრაზებული ხარ და უფრო ადვილია მისთვის ცუდის თქმა, თუ ის ვერ ხვდება, რომ ეს შენ ხარ. ამის გაკეთება ინტერნეტით ზუსტად ისევე საზიანო და მტკივნეულია, როგორც რეალურ ცხოვრებაში.

რასაც ინტერნეტში გამოაქვეყნებ, შეიძლება ხელმისაწვდომი იყოს უცნობებისთვის და მათ არასწორად გაიგონ შენი ნათქვამი. მაშინაც კი, თუ შენ მხოლოდ ხუმრობ. ისინი შეიძლება ვერ ხვდებოდნენ, რომ ეს ხუმრობაა და შეიძლება შენს ნათქვამზე ძალიან განაწყენდნენ, ან გაბრაზდნენ კიდეც.

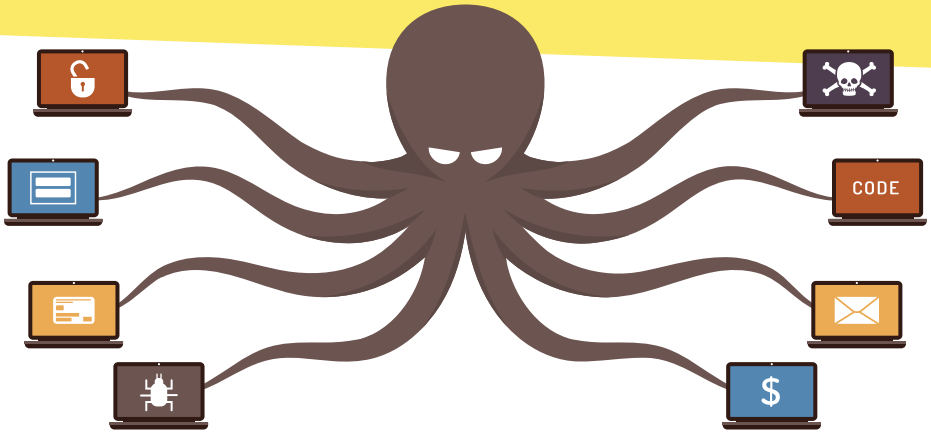
იყავი პოზიტიური ინტერნეტში. რასაც არ იტყოდი პირად საუბარში, ნუ იტყვი ინტერნეტში. და ზუსტად ისევე, როგორც ჩვეულებრივი ბულინგის შემთხვევაში უთხარი უფროსებს თუ შენ ან შენს რომელიმე მეგობარს გაანაწყენებს მსგავსი საქციელი სხვისი მხრიდან.

რა არის მავნე პროგრამები და ვირუსები ?

მავნე პროგრამები მოიცავს ვირუსებს, ჭიებს (Worm) და „ტროას ცხენებს (Trojans)“, ესენი კომპიუტერული პროგრამებია, რომლებსაც შეუძლიათ შენი კომპიუტერისთვის ზიანის მიყენება.

ვირუსი არის პროგრამა, რომელიც ხელს უშლის კომპიუტერის ნორმალურ მუშაობას. ვირუსები ვრცელდებიან ინტერნეტის საშუალებით. ისევე, როგორც ადამიანის ვირუსები, კომპიუტერული ვირუსებიც განსხვავდებიან სიმძიმის მიხედვით, კომპიუტერის ვირუსებიც შეიძლება იყოს მსუბუქად, საშუალოდ და ძალიან დამანგრეველი.

ვირუსს არ შეუძლია ადამიანის ჩარევის გარეშე გავრცელება. ვირუსის გასავრცელებლად ვინმემ უნდა გააგზავნოს ფაილი ან ელექტრონული წერილი.

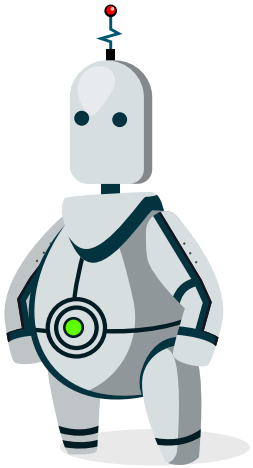


რა არის მავნე პროგრამები და ვირუსები ?

- შედარებით ძლიერ ვირუსებს, მაგ. ჭიებს, შეუძლიათ საკუთარი თავის ავტომატურად წარმოება და სხვა კომპიუტერებზე ან პროგრამებზე კონტროლის დამყარება.

- ზოგიერთი ვირუსი სასარგებლო პროგრამას ჰგავს, და მოტყუების გზით არწმუნებს მომხმარებლებს ჩატვირთონ ის თავის მოწყობილობაში. მას შეუძლია სასარგებლო პროგრამის მსგავსად მოქმედება და ამავდროულად კომპიუტერისთვის ზიანის მიყენება.

- ვირუსებისგან დასაცავად რეგულარულად განაახლე უსაფრთხოების საშუალებები შენს კომპიუტერში.



თამაშზე დამოკიდებულება

რა არის თამაშზე დამოკიდებულება?

რა გავლენას ახდენს კომპიუტერული თამაშები ჯანმრთელობაზე?

კომპიუტერული თამაშები პრაქტიკულად არასოდეს სრულდება, შენ ყოველთვის გადადიხარ ახალ ეტაპზე, და იმის ნაცვლად, რომ ყურადღება რამე სხვა საქმიანობაზე გადაიტანო, მუდმივად იმაზე იფიქრებ, თუ როგორ მოხვდე კომპიუტერთან და რაც შეიძლება მალე განაგრძო საინტერესო თამაში. ამას ეწოდება დამოკიდებულება.

ზოგჯერ, შეიძლება ძალიან სერიოზულად მიიღო თამაშის პროცესი და ჩამოაყალიბო შენი „ვირტუალური სამყარო“, სადაც თავი შენს საყვარელ გმირად წარმოგიდგენია. როდესაც რეალურ ცხოვრებაში უბრალო მოსწავლე ხარ, ვირტუალური სამყარო შენთვის უფრო და უფრო საინტერესო ხდება. ვირტუალურ რეალობაზე გადართვით, სულ უფრო ჩაკეტილი ხდები.

ეს კი ნიშნავს, რომ ვერ ივითარებ კომუნიკაციის უნარს, რომ ნაკლებს ურთიერთობ თანატოლებთან, ვერ სწავლობ კონფლიქტური სიტუაციების გადაწყვეტას, არ ეცნობი გარემომცველ რეალობას. ყოველთვის უნდა გახსოვდეს, რომ ეს მხოლოდ თამაშია, ხოლო მეგობრებთან რეალურ ცხოვრებაში ურთიერთობა ბევრად უკეთესია - იმიტომ, რომ ეს ხდება სინამდვილეში.

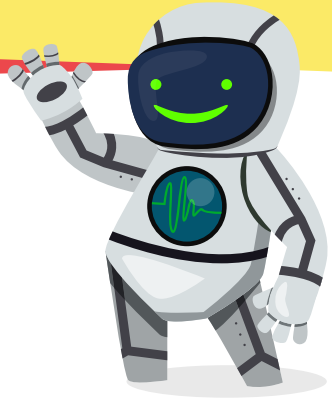
ინტერნეტში ქცევის წესები

წესები, რომელთა დაცვაც აუცილებელია:

- შენს მშობლებს და მასწავლებლებს შეუძლიათ დაგეხმარონ უსაფრთხო საიტების პოვნაში. უამრავ საიტზე შეგიძლია სწავლა და გართობა პროფილის შექმნის გარეშე, თუ რეგისტრაცია დაგჭირდება, უმჯობესია მშობლებს სთხოვო დახმარება. ნება მიეცი მშობლებს დაგეხმარონ და გააკონტროლონ შენი ონლაინ აქტივობა.

- ყურადღებით იყავი, რომ არ გაავრცელო ფოტოები, სადაც არიან სხვა ადამიანები, ან კიდევ ისეთი ფოტოები, რომლებითაც სხვებმა შეიძლება გაიგონ თუ სად იმყოფები კონკრეტულად.

- ზოგიერთმა კომპიუტერმა და ტელეფონმა შეიძლება გაამჟღავნოს შენი ადგილსამყოფელი ისე, რომ შენ არც კი იცოდე ამის შესახებ. სასურველია ყოველთვის გამორთული გქონდეს ადგილმდებარეობის დადგენის ფუნქცია აპლიკაციებში, თუ არ იცი როგორ გამორთო ეს ფუნქცია, დახმარებისთვის მიმართე უფროსებს.



ინტერნეტში ქცევის წესები

ნუ იქნები უხეში ინტერნეტში, ნუ გააღიზიანებ და ნუ მიაყენებ შეურაცხყოფას სხვებს ინტერნეტში. ზუსტად შენს მსგავსად, ისინიც რეალური ადამიანები არიან და მათაც გააჩნიათ გრძნობები.

ყოველთვის თქვი, თუ ონლაინ სივრცეში, უცნაურ ან ცუდ საქციელს შენიშნავ. დაუყოვნებლივ აცნობე უფროსს, თუ უცნობი მოგწერს, ან რაიმე უხერხულობას შეგიქმნის. ასევე უთხარი უფროსს, თუ ვინმე დასცინის ან რამე უცნაურს ეუბნება სხვა ბავშვებს. ბევრ საიტს შეუძლია გამოავლინოს წესების დამრღვევი. მათი გამოყენებით, ან უფროსების (მშობლების ან უფროსი ძმის ან დის) დახმარებით შენ, როგორც საკუთარ თავს ასევე სხვა ბავშვებსაც იცავ.

არ გასცე პირადი ინფორმაცია

Facebook, Instagram და სხვა საიტები მოითხოვენ პროფილის შექმნას, რაც უნდა გააკეთო მშობლების ან ზრდასრულების დახმარებით. რატომ? შენი ინფორმაცია შესაძლოა ისეთი მიზნებისთვის გამოიყენონ, რაც ნამდვილად არ მოგეწონება. მაგალითად უამრავი, უსარგებლო შეტყობინების მიღება.

თუ გაქვს საკუთარი პროფილი სოციალურ ქსელებში და მიიღებ შეტყობინებას, სადაც გთხოვენ პირად ინფორმაციას, მაგალითად ტელეფონის ნომერს, მისამართს ან მშობლების სახელებს, შეატყობინე დედას ან მამას ვიდრე უპასუხებ ამ წერილს. ზოგიერთი შეტყობინება ოფიციალურს წააგავს, მაგრამ ეს უბრალოდ ხრიკია, რათა გამოგტყუონ პირადი ინფორმაცია.

ჯობია შენი სახელისგან განსხვავებული პროფილის სახელის არჩევა. მაგ, „გიორგი“-ს ნაცვლად, ხომ შეიძლება დაირქვა “Sk8boy21”? მხოლოდ შენს მეგობრებს და ოჯახის წევრებს ეცოდინება შენი კოდური სახელი!

სოციალურ ქსელებში ქცევის წესები

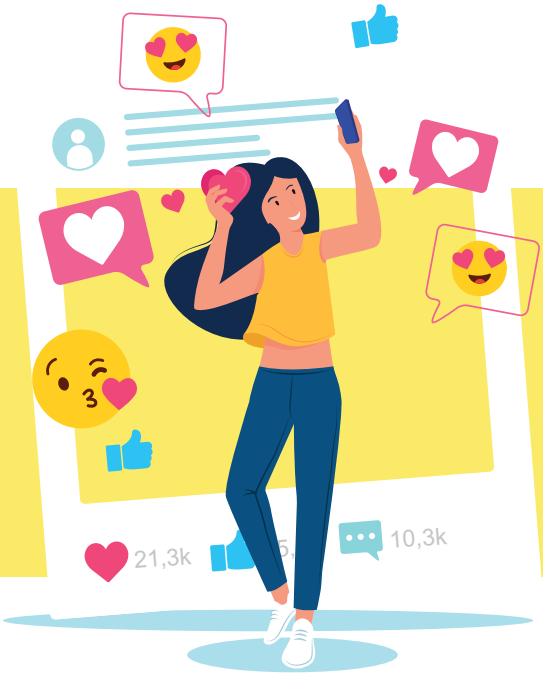
ფოტო: საიტზე არასოდეს ატვირთო ისეთი ფოტო, რომლის გამოც შეიძლება თავი უხერხულად იგრძნო, თუნდაც მშობლების წინაშე. ასევე, ნებართვის გარეშე არ ატვირთო ინტერნეტში შენი მეგობრების ფოტოები. იცოდე, რომ ყველა ფოტოს გადმოწერა შეიძლება და არასოდეს გეცოდინება, თუ სად შეიძლება აღმოჩნდეს შენი სურათები.

პროფილი: პროფილის შედგენისას რაც შეიძლება მოკლე ინფორმაცია შეიყვანე. არ გაამჟღავნო შენი ტელეფონის ნომერი, მშობლების სახელები, საცხოვრებელი მისამართი - ისინი შეიძლება ბოროტად გამოიყენონ შენს წინააღმდეგ.

სოციალურ ქსელებში ქცევის წესები

- ურთიერთობა: არ უპასუხო უსიამოვნო, ან უხამს კომენტარებს. მეგობრებთან ისაუბრე დაფიქრებულად, იცოდე, რომ თქვენი საუბარი შეიძლება ნებისმიერმა წაიკითხოს.

- მეგობრების სიაში დაამატე მხოლოდ ის ადამიანები, ვისაც პირადად იცნობ. მნიშვნელოვანია არა ის, თუ რამდენი ადამიანის დამატებას შეძლებ მეგობრებში, არამედ ის, თუ რამდენი მეგობარი გყავს სინამდვილეში. ყოველთვის გახსოვდეს, რომ ინტერნეტში ყველა შენი გზავნილი ხელმისაწვდომია სხვებისთვის!



უსაფრთხოების წესები ინტერნეტში

- დარწმუნდი, რომ შენს კომპიუტერზე, ტელეფონზე ან პლანშეტზე დაყენებულია ანტივირუსული პროგრამა. ის დაგიცავს ყველაზე მეტად გავრცელებული თავდასხმებისგან.

- არ გადმოწერო ფაილები არასანდო საიტებიდან, უმჯობესია, ისინი შემქმნელის ვებგვერდიდან გადმოწერო. თუ უცნობი საიტიდან გადმოწერილ პროგრამებს დააყენებ, მათთან ერთად შეიძლება რამდენიმე, ძალიან არასასიამოვნო სიურპრიზი-კომპიუტერული ვირუსიც მიიღო.

- თუ პროგრამა უცნობმა გამოგიგზავნა, არ სცადო მისი დაყენება. ვირუსი, პატარა ფაილშიც შეიძლება იყოს ჩასმული, რასაც ცუდი შედეგების გამოწვევა შეუძლია, მაგალითად პაროლების მოპარვა, შენი მოწყობილობიდან ნებისმიერი ფაილის წაშლა ან შენი სახელით სპამის გაგზავნა.

- მაშინაც კი, თუ პროგრამის შემცველი გზავნილი შენი მეგობრის ან ოჯახის წევრისგან მიიღე, უმჯობესია გაარკვიო, ხომ არ გატეხეს მისი პროფილი, ჰაკერები ხომ სხვა ადამიანებად გვაჩვენებენ თავს. ეს მათ უფრო უადვილებს ვირუსების და მავნე პროგრამების გავრცელებას. ამიტომაც არ უნდა გადახვიდე მიღებულ ბმულებზე და არ უნდა დააყენო ინტერნეტით მიღებული ფაილები.

პაროლები და უსაფრთხოება

არსებობს რამდენიმე წესი, რომელთა დაცვაც სასურველია

არავის გაუმხილო შენი სოციალური ქსელების ან ონლაინ თამაშების პროფილის პაროლები. შენს საუკეთესო მეგობარსაც კი. მას შემდეგ, რაც კიბერ დამნაშავე გამოგტყუებს პაროლს, მას შეეძლება ფასეული სათამაშო ელემენტების მოპარვა, ან შენი გვერდის გამოყენება, შენს მეგობრებთან ვირუსების და მომაბეზრებელი სპამის გასაგზავნად. მათ კი, ეს ნამდვილად არ მოეწონებათ!

არასოდეს გადააგზავნო პაროლი ფოსტით ან მესენჯერის ტიპის პროგრამებით, როგორიცაა: Skype, Viber, WhatsApp და სხვა, იმ შემთხვევაშიც კი, თუ ამას მოგთხოვთ სოციალური ქსელის ან სათამაშო სერვისის „თანამშრომელი“. დანამდვილებით შეიძლება ითქვას, რომ არცერთი სოციალური ქსელის ან სათამაშო სერვისის თანამშრომელი არასოდეს არ მოითხოვს შენს პაროლს.

ეცადე გამოიყენო გრძელი და რთული პაროლები: მინიმალური სიგრძე 12 სიმბოლო, დიდი და პატარა ასოების, ციფრების და სასვენი ნიშნების ჩათვლით. პაროლისთვის არ გამოიყენო ისეთი ინფორმაცია რომელიც სხვებმაც იციან ან ციფრების მარტივი კომბინაცია, მაგალითად “12345“. ნაცნობებიც ადვილად შეძლებენ მათ გამოცნობას, ხოლო, კიბერ დამნაშავეებს პაროლის გასატეხად შეუძლიათ სპეციალური პროგრამების გამოყენება. ერთი შეხედვით ეს შეიძლება რთულად მოგეჩვენოს, მაგრამ სინამდვილეში არსებობს საიმედო პაროლის შექმნის მარტივი გზები.

პაროლები და უსაფრთხოება

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

მაშ ასე, როგორ უნდა შეადგინო ადვილად დასამახსოვრებელი და საიმედო პაროლი? ძლიერი პაროლის შედგენის მრავალი გზა არსებობს, მაგრამ ჩვენ გირჩევთ შექმნა პაროლები ასოციაციების გამოყენებით.

#@%^&
()785}&
>CODE@
3#$%<T
678+Y@

პაროლები და უსაფრთხოება

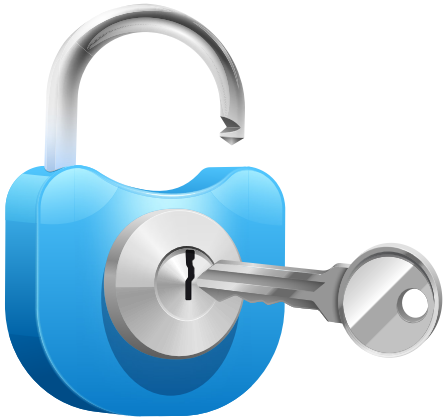
ძლიერი პაროლის შესაქმნელად:

1. გაიხსენე საყვარელი ფრაზა ან სტროფი სიმღერიდან, ფილმიდან ან მულტიპლიკაციური ფილმიდან, რომელიც ძალიან მოგწონს.

2. ჩამოწერე პირველი ხუთი სიტყვის, პირველი ასოები.

3. ყოველ ასოს შორის ჩასვი ერთი სპეციალური სიმბოლო.

ამის შემდეგ შენ მზად გექნება კომბინაცია, რომლითაც მიიღებ უსაფრთხო პაროლს. ერთადერთი, რაც დარჩა გასაკეთებელი, არის იმის გარკვევა, თუ როგორ უნდა გამოიყენო ასოციაციები, რომ ადვილად დაიმახსოვრო თითო პაროლი, თითოეული საიტისთვის.



პაროლები და უსაფრთხოება

როგორი ასოციაციები გიჩნდება, როდესაც ფიქრობ Facebook -ის, Instagram-ის და სხვა საიტების შესახებ, სადაც გსურს დარეგისტრირება? გამოიყენე შექმნილი ასოციაციის პირველი ასო საბაზო კომბინაციის შესადგენად. მაგალითად, თუ სოციალური ქსელი გაგონებს შენი მეგობრების ცეკვას კამერის წინ, მაშინ შეგიძლია გამოიყენო სიტყვა «dance».

ამგვარად, თუ ასოციაციურ ფრაზად ავირჩევთ, მხიარულ სტრიქონს «Twinkle Twinkle Little Star How I Wonder What You Are», ხოლო სპეციალურ სიმბოლოდ, ინსტაგრამის მომხმარებელთა საყვარელ ნიშანს - «#», მაშინ შენი პროფილის პაროლი იქნება «T#T#L#S#Hdance».

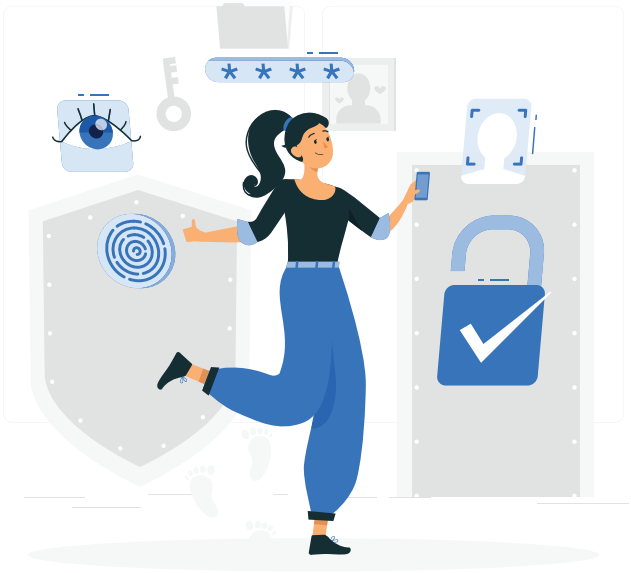
სიმბოლოების ეს კომბინაცია სხვა ნებისმიერი ადამიანისთვის უაზროა, მაგრამ რადგან შენ იცი სისტემა და საიტთან დაკავშირებული პირადი ასოციაციები, ეს პაროლი ადვილი და გასაგები იქნება შენთვის.

პაროლები და უსაფრთხოება

ნუ დაწერ პაროლებს ფურცლებზე და ნუ შეინახავ მათ მყარ დისკზე. კიბერ დამნაშავე სწორედ აქ დაიწყებს მათ ძებნას. პაროლის შენახვის საუკეთესო გზა, მისი დამახსოვრებაა.

პაროლის შეყვანისას დარწმუნდი, რომ ეს სწორედ ის საიტია, რომელიც გჭირდება. კიბერ დამნაშავეები მომხმარებლების პაროლების მოპარვის მიზნით ხშირად აკეთებენ პოპულარული საიტების ასლებს.

ვებ საიტის სანდოობის გადამოწმების ყველაზე მარტივი გზა საიტის მისამართის ყურადღებით წაკითხვაა.



პაროლები და უსაფრთხოება

გამოიყენე საიმედო პაროლები! აზრი, რომ პაროლების დამახსოვრება ძნელია, არა მხოლოდ მცდარია, არამედ სახიფათოცაა!

ყოველთვის გახსოვდეს ეს ოქროს 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.
- მოიფიქრე პაროლები ისეთ ფრაზებზე დაყრდნობით, რომლებიც შენთვის რაღაცას ნიშნავს და შენ ადვილად დაიხსომებ მათ!
- სხვისი კომპიუტერის გამოყენებისას გათიშე პაროლის დამახსოვრების ფუნქცია, წინააღმდეგ შემთხვევაში შენი პაროლი შეინახება სხვის კომპიუტერში.

ლექსიკონი

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

ანტივირუსი - არის 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 - არის 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) - გულისხმობს ფიზიკურ ან სოციალურ ძალადობას, რომელიც იწვევს ზიანს, შიშს და/ან მწუხარებას. იგი მოქმედებს ადამიანის ემოციურ მდგომარეობაზე და ლახავს მის რეპუტაციას.

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

ლექსიკონი

კიბერბულინგი - შეურაცხყოფის შემცველი შეტყობინებებით, აგრესიით, დაშინებით შევიწროება და ხულიგნობა, სხვადასხვა ინტერნეტ სერვისების 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.

სპამი - წერილების გაგზავნა მიმღების თანხმობის გარეშე.

ჰაკერი - ადამიანი რომელიც იყენებს ტექნოლოგიებს საიტების ან სხვა სისტემების გასატეხად. ხშირად ჰაკერები თავისი ქმედებისთვის ვირუსებსაც იყენებენ.