ინტერნეტში უსაფრთხოების გზამკვლევი ბავშვებისთვის

ასაკი: 12-18 წელი

World Vision

მაქსიმ იავიჩი
გიორგი იაშვილი

2020

სარჩევი

შესავალი ინტერნეტ უსაფრთხოებაში

ინტერნეტი მთელს მსოფლიოში კომუნიკაციის და ინფორმაციის სწრაფად მიღების საშუალებას გვაძლევს, თუმცა გარკვეულ რისკებსაც შეიცავს, როგორიცაა, მაგალითად: მავნე პროგრამა, "სპამი" და "ფიშინგი". თუ ინტერნეტის უსაფრთხოდ გამოყენება გსურს, კარგად უნდა იცნობდე შესაძლო საფრთხეებს. ინტერნეტში ყოფნისას შესაძლოა უსაფრთხოების ყალბი შეგრძნება გაგიჩნდეს, რადგან კომპიუტერის ეკრანიდან ფიზიკურ ზიანს ვერავინ მოგაყენებს. მაგრამ იმისათვის, რომ ინტერნეტში უსაფრთხოდ იყო მეტი ყურადღება გმართებს.

ინტერნეტით სარგებლობამ არ უნდა შეგაშინოს, მაგრამ უნდა გახსოვდეს, რომ იქ ზუსტად ისეთივე საფრთხის წინაშე შეიძლება აღმოჩნდე, რაც რეალურ ცხოვრებაში გვხვდება. ამ გზამკვლევში გიჩვენებთ, როგორ მოემზადო ამ რისკებისთვის, ისე, რომ ინტერნეტ სივრცეში ყოფნისას საფრთხისგან დაცული იყო.

შენი იდენტობა ონლაინ სივრცეში

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

რა უნდა გავითვალისწინოთ ონლაინ იდენტობისა და რეპუტაციის დასაცავად:

გახსოვდეს, რომ ონლაინში არაფერია დროებითი: ონლაინ სამყაროში არსებობს სხვებთან ურთიერთობის დამყარების და ინფორმაციის გაზიარების უამრავი გზა. ეს არის ადგილი, სადაც დროებითი არაფერია და განხორციელებული ქმედებების უკან დაბრუნება შეუძლებელი. გაზიარებული ინფორმაციის უმეტესი ნაწილი რჩება ინტერნეტ სივრცეში სამუდამოდ.

შენი იდენტობა ონლაინ სივრცეში

შენი პროფილი არ უნდა იყოს ღია ყველასთვის: შენს სოციალური ქსელის გვერდზე შემოსულ ნებისმიერ პირს შეუძლია, ისეთი ინფორმაციის გადმოწერა, რის საჯაროდ გავრცელებასაც არ მოისურვებდი. გაეცანი თითოეული საიტის წესებს და პირობებს და დარწმუნდი, რომ შენი პირადი ინფორმაცია უცნობებისთვის მიუწვდომელია.

ხშირად შეცვალე პაროლები: თუ ვინმე შეძლებს შენს გვერდზე შეღწევას, მას შეეძლება შენ მაგივრად ფოტოების ატვირთვა, შენი სახელით შეტყობინებების გაგზავნა ან პროფილის მითვისება და წაშლაც კი. შეარჩიე პაროლები, რომლებსაც ვერავინ გამოიცნობს და ხშირად ცვალე ისინი. მშობლების გარდა არავის გაუზიარო შენი პაროლები.

შენი იდენტობა ონლაინ სივრცეში

არ გამოაქვეყნო გამომწვევი სურათები ან კომენტარები. რაც ახლა სასაცილოდ ან სასიამოვნოდ მიგაჩნია, შეიძლება არც ისე სასიამოვნო აღმოჩნდეს წლების შემდეგ - ან როდესაც მასწავლებელი ან პოტენციური დამსაქმებელი ნახავს მათ. არ ღირს ისეთი ფოტოების გამოქვეყნება, რომელთა გამოც თავს უხერხულად იგრძნობდი, თუ მათ შენი ბებია, მასწავლებელი ან საუკეთესო მეგობრის მშობლები ნახავდნენ; მაშინაც კი, თუ ეს სურათები მხოლოდ შენს პირად გვერდზეა განთავსებული.

არ უპასუხო შეუსაბამო მოთხოვნებს. ბევრი არასრულწლოვანი ინტერნეტში იღებს შეუსაბამო მოთხოვნებს და შეთავაზებებს. ეს შეიძლება უცნაური, უხერხული და საშიშიც კი იყოს. თუ ინტერნეტში უცნობის ან მეგობრის მხრიდან თავს შევიწროებულად იგრძნობ, დაუყოვნებლივ უთხარი მშობლებს ან უფროსებს. პასუხის გაცემას არასოდეს მოაქვს კარგი შედეგი, ამან შეიძლება უფრო დაამძიმოს მდგომარეობა ან ისეთი რამ გათქმევინოს რის გამჟღავნებასაც არ ისურვებდი.

არ იჩქარო გამაღიზიანებელ შეტყობინებაზე პასუხის გაცემა. თუ ინტერნეტით გამაღიზიანებელ შეტყობინებას მიიღებ, არ იჩქარო პასუხის გაცემა. ყოველთვის სჯობს დამშვიდდე და მხოლოდ ამის შემდეგ გადაწყვიტო როგორ მოიქცე. დამშვიდებულზე შეძლებ, სხვანაირად შეხედო სიტუაციას.

შენი იდენტობა ონლაინ სივრცეში

გახსოვდეს, უმჯობესია არ გამოაქვეყნო ან არ გააგზავნო ინტერნეტით ისეთი რამ, რასაც არ იტყოდი ან ჩაიდენდი სხვების თანდასწრებით.

პატივი ეცი საავტორო უფლებებს. არსებობს კანონი საავტორო უფლებების შესახებ. დარწმუნდი, რომ არ აქვეყნებ საავტორო უფლებებით დაცულ ფაილებს. არ ღირს ისეთი რაიმეს გამოქვეყნება, რაც კანონს ეწინააღმდეგება და რაზეც მოგვიანებით, შესაძლოა, პასუხი მოგთხოვონ.

შეამოწმე შენი თავი ინტერნეტ სივრცეში. სცადე შენი ზედმეტსახელის ან ელექტრონული ფოსტის მისამართის მოძებნა საძიებო სისტემების საშუალებით. ამგვარად შენ ნახავ თუ როგორ გხედავენ ინტერნეტში. თუ გაგიჩნდება შეკითხვები იმ კვალის შესახებ, რასაც ინტერნეტში ტოვებ, მიმართე უფროსებს. შესაძლოა, მათთან შედარებით უკეთ იცნობდე ონლაინ სამყაროს, მაგრამ არსებობს სიტუაციები, როდესაც მათი ცოდნა და გამოცდილებაც დაგეხმარებათ.

კიბერბულინგი

კიბერბულინგიბულინგის სახეობა, რომელიც ონლაინ სივრცეში ხორციელდება შეურაცხყოფის შემცველი შეტყობინებებით, აგრესიით, დაშინებით, სხვადასხვა ინტერნეტსერვისების საშუალებით. გამომგზავნი შეიძლება უცნობი ადამიანი ან ყოფილი მეგობარიც კი იყოს. კიბერბულინგი შეიძლება შეიცავდეს ფოტოებს, შეტყობინებებს ან გვერდებს, რომელთა წაშლა შეუძლებელია. ერთი სიტყვით, ეს არის ყველაფერი, რაც ინტერნეტში ქვეყნდება სხვისი ჩაგვრის, შევიწროების, განაწყენების და ზიანის მიყენების მიზნით.

კიბერ ხულიგნები, სხვა ხულიგნების მსგავსად, შენს რეაქციას ელოდებიან და ყურადღების მიქცევას ცდილობენ. მათი პროვოცირება არასოდეს არის მიზანშეწონილი. იგნორირებით ისინი ზეგავლენას კარგავენ. შენ ასევე შეგიძლია წაშალო ან დაბლოკო ხულიგნები რომ აღარ მოგივიდეს მათი შეტყობინებები.

სქესთან, რელიგიასთან, სექსუალურ ორიენტაციასთან დაკავშირებული უხეში კომენტარები, დაცინვა, დაშინება და სხვა სახის დისკრიმინაცია ქვეყნების უმრავლესობაში კანონდარღვევად ითვლება, რაც საქმეში პოლიციის ჩართვის შესაძლებლობას იძლევა. ამ გზით შეძლებთ შეაჩეროთ კიბერ ხულიგნები და თავი დაიცვათ მათგან.

კიბერბულინგი

ზოგჯერ, ონლაინ ბულინგმა, სხვა სახის ბულინგის მსგავსად შეიძლება სერიოზულ პრობლემებამდე მიგვიყვანოს. მუდმივმა სტრესმა და შიშმა შეიძლება გამოიწვიოს განწყობის, ენერგიის, ძილისა და მადის დაქვეითება, აგრეთვე, საკმაოდ მძიმე ფსიქოლოგიური პრობლემები.

კიბერბულინგმა შესაძლოა სერიოზული პრობლემები შეუქმნას მის განმახორციელებლებსაც: სულ უფრო მეტი სასკოლო და არასასკოლო პროგრამა ქმნის კიბერბულინგზე რეაგირების სისტემებს. კიბერ ხულიგნები სკოლებმა სპორტული გუნდებიდან და სკოლიდანაც კი შეიძლება გარიცხონ. კიბერბულინგის ზოგიერთი სახეობა შეიძლება არღვევდეს სკოლის წესებს ან დაარღვიოს ანტიდისკრიმინაციული ან სექსუალური შევიწროების კანონები. ასე რომ, ხულიგანს შესაძლოა სერიოზული კანონდარღვევების გამო მოუწიოს პასუხისგება.

კიბერბულინგი

ზოგჯერ, ადამიანებს ეშინიათ ან არ არიან დარწმუნებულები, რომ მათ აბულინგებენ. ამიტომ ისინი არაფერს აკეთებენ საპასუხოდ. თუ ვინმე შენ ან შენს ნაცნობს აბულინგებს, ავიწროებს ან ცდილობს ზიანი მიაყენოს, ჩუმად არ უნდა იყო, უნდა დაარეპორტო აბსოლუტურად ყველა შემაშფოთებელი შეტყობინება ან პოსტი.

გაანდე ვინმეს: კიბერბულინგის შემთხვევების აღმოჩნისას, უპირველეს ყოვლისა, შეგიძლიათ მიმართოთ უფროსებს. ზოგჯერ ამის თქმა უფრო ადვილია ვიდრე გაკეთება. ხშირ შემთხვევაში, ბულინგის მსხვერპლს ეუხერხულება საუბარი აღნიშნულთან დაკავშირებით. ზოგიერთი შეიძლება ყოყმანობდეს, ვინაიდან არ იცის ვინ არის ხულიგანი. უმრავლეს შემთხვევაში, პოლიციას შეუძლია ბულინგის განმახორციელებლის კვალის პოვნა, ასე რომ, მსგავსი შემთხვევების აღმოჩენისას შესაძლებელია მათი დახმარების გამოყენებაც.

კიბერბულინგი

ზოგიერთი მშობელი საკუთარი შვილის კიბერბულინგისაგან დასაცავად რადიკალურ ზომებს მიმართავს ტელეფონის, კომპიუტერის ჩამორთმევის გზით. თუკი თავს ბულინგის მსხვერპლად თვლი, მაგრამ მშობლებისათვის ამის გამხელისაგან თავს იკავებ, გახსოვდეს, რამდენად სერიოზულ საკითხს ეხება საქმე! შეეცადე გაესაუბრო მშობლებს კიბერბულინგის შემთხვევაზე და მათთან ერთად მოძებნო გამოსავალი, როგორ შეიძლება არსებული პრობლემის მოგვარება ინტერნეტთან (ტელეფონთან, კომპიუტერთან) წვდომის შეზღუდვის გარეშე.

დაბლოკე ხულიგანი: გარდა ამისა გაჯეტების უმეტესობას აქვს პარამეტრები რომელთა დახმარებითაც შეძლებ კიბერ ხულიგნის დაბლოკვას, რომ აღარ მოგივიდეს მისგან შეტყობინებები. თუ თავად ვერ შეძლებ ამის გაკეთებას, უფროსს ან მეგობარს სთხოვე დახმარება.

კიბერბულინგი

თუ შენი მეგობარი კიბერ ხულიგანია:

თუ იცი, რომ შენი მეგობარი იქცევა როგორც კიბერ ხულიგანი, შეარჩიე მომენტი და პირადად ესაუბრე მას. იყავი პრინციპული. შენმა მეგობარმა უნდა იცოდეს, რომ ეს არ არის კარგი საქციელი, აუხსენი მას, რომ ამას შეიძლება სერიოზული შედეგები მოჰყვეს არა მხოლოდ მისთვის, არამედ ისეთი მოწმეებისთვისაც, როგორიც შენ და შენი მეგობრები არიან.

რა არის თამაშზე დამოკიდებულება ?

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

ზოგჯერ, შეიძლება ძალიან სერიოზულად მიიღო თამაშის პროცესი და ჩამოაყალიბო შენი „ვირტუალური სამყარო", სადაც თავი შენს საყვარელ გმირად წარმოგიდგენია. როდესაც რეალურ და ვირტუალურ სამყაროში მოვლენები და გარემოებები ერთმანეთისაგან განსხვავებული ხდება, სულ უფრო ჩაკეტილი ხდები, იწყებ ცხოვრებას ვირტუალური რეალობით.

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.

რისთვის გჭირდება ძლიერი პაროლი ?

ონლაინში აბსოლუტურად ყველაფრისთვის გჭირდება პაროლი. თამაშებიდან დაწყებული, ელექტრონული ფოსტით დამთავრებული. რამდენადაც ადვილია, იოლად დასამახსოვრებელი, მოკლე პაროლების გამოყენება, იმდენად დიდი რისკის ქვეშ დგას შენი ონლაინ უსაფრთხოება. შენი თავის და ინფორმაციის დასაცავად აუცილებელია გრძელი, ძლიერი და სხვისთვის ძნელად გამოსაცნობი, მაგრამ შენთვის იოლად დასამახსოვრებელი პაროლი.

რისთვის გჭირდება ძლიერი პაროლი ?

შეიძლება იკითხო „საერთოდ რა საჭიროა ეს ძლიერი პაროლი?“ მიუხედავად იმისა, რომ ვებგვერდების უმეტესობა უსაფრთხოა, მაინც არის იმის მცირედი შანსი, რომ ვინმემ სცადოს შენს პროფილში შესვლა ან შენი ინფორმაციის მოპარვა. ეს საყოველთაოდ ცნობილია, როგორც კიბერდანაშაული. ძლიერი და საიმედო პაროლი - შენი პროფილის და პირადი ინფორმაციის ჰაკერებისგან დაცვის საუკეთესო გზაა.

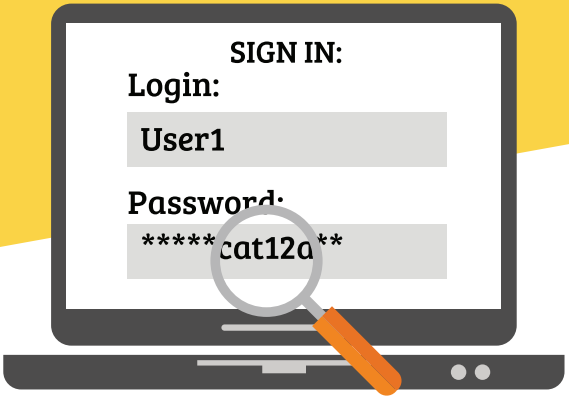
პაროლი შეიძლება სახლის გასაღებს შევადაროთ. ყველამ იცის, რომ არ შეიძლება უცნობისთვის გასაღების მიცემა, ვინაიდან ის ნებართვის გარეშე შეძლებს თქვენს სახლში შემოსვლას. ასევე პაროლი შეიძლება შევადაროთ კბილის ჯაგრისს, ის უნდა შეიცვალოს ყოველ 3-4 თვეში, რადგან ის ძველდება და კარგავს ეფექტურობას.

რისთვის გჭირდება ძლიერი პაროლი ?

პირველ რიგში ზარალდება ის, ვინც არ ზრუნავს საკუთარ უსაფრთხოებაზე ონლაინში. ინტელექტი და ცოდნა საუკეთესო იარაღია კიბერ დამნაშავეების წინააღმდეგ.

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!



რისთვის გჭირდება ძლიერი პაროლი ?

არ 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 სოციალური ქსელის ან სათამაშო სერვისის თანამშრომელი არასოდეს 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.

რისთვის გჭირდება ძლიერი პაროლი ?

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

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

რისთვის გჭირდება ძლიერი პაროლი ?

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 ჩაამატე ერთი სპეციალური სიმბოლო.

ამის შემდეგ შენ მზად გექნება კომბინაცია, რომლითაც მიიღებ უსაფრთხო პაროლს.

რისთვის გჭირდება ძლიერი პაროლი ?

ერთადერთი, რაც დარჩა გასაკეთებელი, არის იმის გარკვევა, თუ როგორ უნდა გამოიყენო ასოციაციები, რომ ადვილად დაიმახსოვრო თითო პაროლი, თითოეული საიტისთვის.

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».

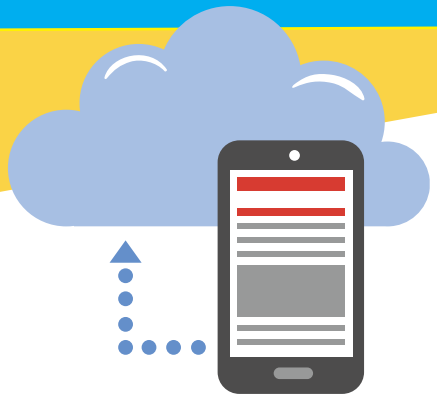
რისთვის გჭირდება ძლიერი პაროლი ?

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

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.



რისთვის გჭირდება ძლიერი პაროლი ?

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

ყოველთვის გახსოვდეს 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.
- 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.

მავნე პროგრამები

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. 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.

მავნე პროგრამები

რა არის არასასურველი პროგრამა? არასასურველი პროგრამები შენი თანხმობის გარეშე ასრულებენ დავალებებს შენს კომპიუტერში. მათ შეიძლება გიჩვენონ რეკლამები, განცხადებები ან შეაგროვონ პირადი ინფორმაცია შენზე და შენს ოჯახზე.

როგორ უნდა მიხვდე, რომ შენი კომპიუტერი დავირუსდა? შენი კომპიუტერის მუშაობა შესაძლოა შენელდეს. ზოგჯერ ვირუსი კომპიუტერის ჩართვაზე პასუხისმგებელ ფაილებსაც აზიანებს. ამ დროს კომპიუტერის ჩამრთველ ღილაკზე დაჭერისას, ეკრანზე ვერაფერს დაინახავ. ყველა ეს სიმპტომი არის კომპიუტერის ვირუსით დაინფიცირების ტიპიური ნიშანი, თუმცა ასეთივე ნიშნები შეიძლება გამოიწვიოს აპარატული ნაწილის ან პროგრამული უზრუნველყოფის პრობლემებმაც, რასაც არაფერი აქვს საერთო ვირუსთან.

რჩევა: გახსოვდეს, დავირუსებული ფაილის გახსნის და გაშვების დროს, შეიძლება მაშინვე ვერ გაიგო, რომ მავნე პროგრამა მიიღე, რადგანაც ვირუსები თავიანთ დამანგრეველ საქმიანობას გაშვებისთანავე არ იწყებენ.

თაღლითობა ინტერნეტში და თავდაცვა

რა არის თაღლითობა? ინტერნეტ-თაღლითობათა შორის ფართოდაა გავრცელებული „ფიშინგი“, რაც იმაში მდგომარეობს, რომ ყალბ ელექტრონულ წერილში ჩასმულია პოპულარულ საიტზე გადასასვლელი ბმული, რომელსაც სინამდვილეში მომხმარებელი გადაჰყავს ყალბ ვებგვერდზე, რომელიც ზუსტად ისევე გამოიყურება, როგორც ოფიციალური გვერდი. მას შემდეგ, რაც მომხმარებელს დაარწმუნებენ, რომ ის ნამდვილად ოფიციალურ საიტზე მოხვდა, ჰაკერები ცდილობენ შეაყვანინონ მას პაროლები, საკრედიტო ბარათის მონაცემები ან სხვა საიდუმლო ინფორმაცია, რაც შემდეგ მომხმარებლის საზიანოდ იქნება გამოყენებული.

გარდა ამისა, თუ მშობლები ან ბავშვები მომსახურების ან საქონლის ღირებულების გადახდისას სარგებლობენ საბანკო ბარათით, მნიშვნელობა არა აქვს ეს ინტერნეტით მოხდება, ტელეფონით თუ მაღაზიაში, ისინი დაუცველები არიან თაღლითებისგან. რადგან საბანკო ბარათით შესრულებული ნებისმიერი ოპერაციისას, კომპანიამ საქონლის ან მომსახურების მიწოდებამდე უნდა შეამოწმოს ანგარიშთან დაკავშირებული ინფორმაცია. ეს ინფორმაცია კი დიდ სერვერებზე ინახება. სამწუხაროდ ჰაკერებს შეუძლიათ ასეთი სისტემის გატეხვა და ამ ინფორმაციის მოპოვება.

თაღლითობა ინტერნეტში და თავდაცვა

როგორ მოქმედებენ დამნაშავეები ინტერნეტში

ბოროტმოქმედები ყველაზე ხშირად ონლაინ ჩატების, ელექტრონული ფოსტის ან ფორუმების საშუალებით ამყარებენ ბავშვებთან კონტაქტს, საკუთარი პრობლემების გადასაჭრელად ბევრი მოზარდი მიმართავს ფორუმებს. ბოროტმოქმედები კი ძირითადად აქ არიან ჩასაფრებულები.

ისინი მოზარდის მიზიდვას ცდილობენ ყურადღებით, მზრუნველობით, სიკეთით და საჩუქრებითაც კი, ხშირად დიდ დროს, ფულსა და ენერგიასაც ხარჯავენ ამისთვის. მათ ჩვეულებრივ კარგად იციან მუსიკის სიახლეები და ბავშვების თანამედროვე ინტერესები. ისინი უსმენენ და თანაუგრძნობენ მოზარდებს.

თანდათან მოსაუბრე სულ უფრო ხშირად იყენებს სექსუალური შინაარსის ფრაზებს ან ცდილობს ეროტიული მასალა აჩვენოს ახალგაზრდას. ზოგიერთი მოძალადე უფრო სწრაფადაც მოქმედებს და ცდილობს დაუყოვნებლივ წამოიწყოს ინტიმურ თემებზე საუბარი.

თაღლითობა ინტერნეტში და თავდაცვა

როგორ უნდა დაიცვა თავი

გამოიყენე ბრაუზერის უსაფრთხოების პარამეტრები

ყოველთვის, როცა ინტერნეტში შედიხარ და რამეს ათვალიერებ ან ეძებ, შენი კომპიუტერი სხვადასხვა საფრთხეებს აწყდება მაგ: ვირუსებს, მავნე და ჯაშუშ პროგრამებს. კარგი ამბავი ის არის, რომ შენი კომპიუტერის დასახმარებლად ბრაუზერს უამრავი უსაფრთხოების ფუნქცია აქვს ჩაშენებული. გავეცნოთ რამდენიმე ყველაზე მნიშვნელოვან ფუნქციას, აქვეა რამდენიმე მარტივი რჩევა, რომლებიც გამოგადგება ინტერნეტში უსაფრთხოების უზრუნველსაყოფად.

შეამოწმე ვებ მისამართი

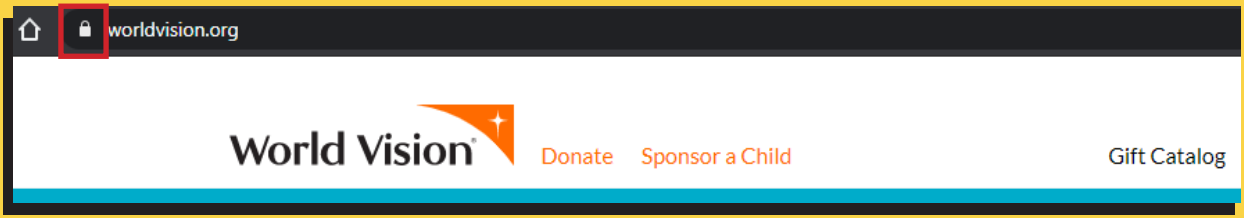
მავნე ვებსაიტები მომხმარებლის შეცდომაში შეყვანის მიზნით, ხშირად იყენებენ მატყუარა ვებ მისამართებს. მაგალითად: www.worldvision.org ისევე გამოიყურება, როგორც www.worldvislon.org, მაგრამ მეორე მაგალითში i -ს ნაცვლად არის l.

თაღლითობა ინტერნეტში და თავდაცვა

ვებ გვერდის სახელის ყურადღებით შემოწმება კარგი გზაა იმაში დასარწმუნებლად, რომ ნამდვილად სასურველ გვერდზე ხარ და არა მიმსგავსებული მისამართის მქონე ყალბ საიტზე.

დააკვირდი უსაფრთხოების სიმბოლოს

ზოგიერთი ვებგვერდის სამისამართო ზოლში ჩნდება ბოქლომის სიმბოლო. ეს ნიშნავს, რომ ვებგვერდი იყენებს დაცულ კავშირს, რაც უზრუნველყოფს პირადი მონაცემების უსაფრთხოებას. თუკი სამისამართო ზოლში არ ჩნდება ბოქლომი, უნდა იცოდე, რომ ასეთ საიტზე არ უნდა შეიყვანო პირადი ინფორმაცია, მაგ: საბანკო ბარათის ნომერი, პაროლი ან პირადი ნომერი.



თაღლითობა ინტერნეტში და თავდაცვა

რეგულარულად განაახლე შენი ბრაუზერი

მუდმივად იქმნება ახალი ვირუსები და მავნე პროგრამები, ამიტომაა აუცილებელი ბრაუზერის რეგულარული განახლება. ბრაუზერი ჩვეულებრივ გაცნობებს, როდესაც ახალი განახლება გამოდის.

თავიდან აიცილე სპამი და ფიშინგი

ინტერნეტი არის კომუნიკაციის ძირითადი საშუალება. სამწუხაროდ ის, ასევე პოპულარულია თაღლითებსა და კიბერდამნაშავეებს შორის. ფიშინგის, მავნე პროგრამებისა და პირადი მონაცემების მოპარვისგან თავის დასაცავად, საჭიროა იცოდე თუ როგორ ამოიცნო და აიცილო თავიდან საფრთხის შემცველი წერილები სპამისა და ფიშინგის მცდელობების ჩათვლით.

თაღლითობა ინტერნეტში და თავდაცვა

სპამ ფილტრები

როდესაც ელ. ფოსტაზე შეტყობინება შემოგდის, იმეილ პროვაიდერების უმეტესობა ამოწმებს ეს სპამია, თუ რეალური შეტყობინება. ყველა საეჭვო შეტყობინება განთავსდება სპამ განყოფილებაში. ამ გზით შენ შეძლებ თვიდან აიცილო სპამ შეტყობინების შემთხვევით გახსნის რისკი.

სპამის ბლოკირების სისტემები სრულყოფილი არ არის, ზოგჯერ საჭირო შეტყობინებაც ხვდება სპამ განყოფილებაში, ამიტომ უმჯობესია რეგულარულად შეამოწმო სპამ განყოფილებაც, რომ არ დაკარგო მნიშვნელოვანი შეტყობინება.

ზოგიერთ საფოსტო სერვისს აქვს ფუნქცია, რომლის საშუალებითაც შესაძლებელია სპამ იმეილების მონიშვნა. მაგალითად: Gmail-ში შეგიძლია შეარჩიო შეტყობინება და დააჭირო ღილაკს „მონიშნე როგორც სპამი“. ეს დაეხმარება შენს ელფოსტის პროვაიდერს ამ ტიპის შეტყობინებების გაფილტვრაში.

თაღლითობა ინტერნეტში და თავდაცვა

სურათები და ფაილები ელ-ფოსტაზე

სპამ შეტყობინებები ხშირად შეიცავენ სურათებს, გამომგზავნს შეუძლია მათთვის თვალყურის დევნება. როდესაც ასეთ შეტყობინებას გახსნი, სურათი ჩაიტვირთება და გამომგზავნს შეატყობინებს, რომ შენი ფოსტა მუშაობს, რასაც კიდევ უფრო მეტი სპამის გამოწვევა შეუძლია. ამის თავიდან აცილებას შეძლებ, თუ დაბლოკავ ფოსტით შემომავალ სურათებს. მაგალითად Gmail-ის პარამეტრებში არსებობს "Ask before displaying external images" ფუნქცია, რომლის აქტივაციის დროს სურათები ჩაიტვირთება მხოლოდ შენი თანხმობის შემდეგ.

სპამი და ფიშინგი ფართოდ გავრცელებული პრობლემაა, მაგრამ ამათ გარდა ელექტრონული ფოსტით თაღლითობის სხვა უამრავი გზა არსებობს. ზოგიერთი თაღლითი შეიძლება დიდი თანხის მოცემას დაგპირდეს, თუ წინასწარ მცირე თანხას გადაუგზავნი. სხვებმა შეიძლება ნაცნობად მოგაჩვენონ თავი და ფულის სესხება ან გამოგზავნილი ფაილის გახსნა გთხოვონ.

გახსოვდეს, ისევე, როგორც სპამისა და ფიშინგის დროს, აუჩქარებლად იმოქმედე. არავის უნდა გაუგზავნო ფული მხოლოდ იმიტომ, რომ ელ.ფოსტით მიიღე მოთხოვნა. ასევე არასოდეს არ უნდა ჩამოტვირთო ელ. ფოსტით მიღებული დანართები, რომლებსაც არ ელოდებოდი, რადგან ისინი შეიძლება შეიცავდნენ მავნე პროგრამებს, რომელთაც შეუძლიათ შენი კომპიუტერის დაზიანება და პირადი ინფორმაციის მოპარვა.

თაღლითობა ინტერნეტში და თავდაცვა

სპამი, თაღლითობა და ფიშინგი მუდმივად განაგრძობს განვითარებას და სახეცვლილებას. მაგრამ როდესაც უკვე იცი, თუ რას მიაქციო ყურადღება და რას აარიდო თავი, შენი კომპიუტერი ბევრად უფრო უსაფრთხოდ იქნება.

როგორ ავიცილოთ თავიდან მავნე პროგრამები

მავნე პროგრამები ფართოდაა გავრცელებული, მაგრამ სინამდვილეში მათგან თავის დაცვა არც ისე რთულია. ინტერნეტში მუშაობის სწორი ჩვევების გამომუშავება დაგიცავს მავნე პროგრამებისა და სხვა საფრთხეებისგან.

დაიცავი შენი კომპიუტერი

კომპიუტერის დაცვა შეგიძლია ანტივირუსით და მავნე პროგრამების საწინააღმდეგო საშუალებებით, როგორიცაა Bitdefender ან Norton. ეს პროგრამები ბლოკავენ მსგავს პროგრამებს და არ აძლევენ მათ კომპიუტერში ჩატვირთვის საშუალებას, ასევე შეუძლიათ მათი წაშლა, თუ ისინი მოხვდებიან სისტემაში.

ბევრი მავნე პროგრამა იყენებს ვინდოუსის და სხვა პროგრამების დაცვის სუსტ მხარეებს. ოპერაციული სისტემის, ბრაუზერის და სხვა პროგრამების განახლება - შენი კომპიუტერის დაცვის საწინდარია.

თაღლითობა ინტერნეტში და თავდაცვა

გააკეთე ფაილების სარეზერვო ვერსია

ზოგიერთმა მავნე პროგრამამ შეიძლება წაშალოს ან დააზიანოს შენს დისკზე განთავსებული მონაცემები. მათი დაკარგვის თავიდან არიდება ბევრად უფრო ადვილი და იაფია ვიდრე მავნე პროგრამის თავდასხმის შემდეგ მათი აღდგენა. ამის ყველაზე მეტად გავრცელებული გზებია მონაცემების დამატებითი ასლების გარე მყარ დისკზე შენახვა ან სარეზერვო კოპირების ონლაინ სერვისის გამოყენება. ფაილების შენახვის ერთ-ერთი კარგი რესურსია Google Drive.

მოერიდე საეჭვო ბმულებს

მავნე პროგრამების უმეტესობა მოითხოვს ბმულზე გადასვლას, ჩამოტვირთვას და ინსტალაციას. ეს ბმულები ხშირად შენიღბულია სასარგებლო პროგრამების სახით. თუ შენ იცი, როგორ შეიძლება გამოიყურებოდნენ საეჭვო ბმულები შეძლებ მათგან თავის არიდებას.

თაღლითობა ინტერნეტში და თავდაცვა

ქვემოთ მოყვანილია შეცდომაში შემყვანი ბმულების მაგალითები, რომლებშიც დამალულია მავნე პროგრამების ჩამოტვირთვის ბრძანება.

- ვებსაიტებზე განთავსებული რეკლამები შეიძლება ჰგავდეს სისტემურ შეტყობინებებს ან დიაგნოზს, რომელიც გაფრთხილებს, რომ შენს კომპიუტერში რაღაც რიგზე არ არის.
- განცხადებები შეიძლება გამოიყურებოდნენ, როგორც შეტყობინება, სადაც ნათქვამია, რომ შენ მოიგე პრიზი და მის მისაღებად უნდა დააჭირო ბმულს.
- მოულოდნელად გამოსული ფანჯრები ხშირად შეიცავენ მავნე პროგრამებს ან ცდილობენ გადაგიყვანონ ნაკლებად უსაფრთხო საიტზე. სანდო ვებგვერდების უმეტესობა არ იყენებს ასეთ „pop-up“ ფანჯრებს, ხოლო ზოგიერთი ბრაუზერი კი საერთოდ ბლოკავს მათ.

თაღლითობა ინტერნეტში და თავდაცვა

- თუ ისეთი ფაილის, ჩამოტვირთვას გთხოვენ, რომლის მიღებასაც არ ელოდი, ან მიგაჩნია, რომ ეს ფაილი არ არის კავშირში იმ საიტთან რომელზეც ხარ, სავარაუდოდ ეს მავნე პროგრამა იქნება.

- სათაურები, რომლებიც ორაზროვანი და სენსაციურია, რომლებიც მოგიწოდებენ ბმულზე გადასვლისკენ, დაწვრილებითი ინფორმაციის მისაღებად, ასეთ საიტებს ეწოდება „clickbait“ საიტები, რომლებიც ხაფანგად იყენებენ უამრავ მიმზიდველ სათაურს, სადაც დამალულია მავნე პროგრამებზე გადასასვლელი ბმულები.

თაღლითობა ინტერნეტში და თავდაცვა

საეჭვო საიტების იდენტიფიცირება

- თუ არ ხარ დარწმუნებული, რომ ვებსაიტი ან ჩამოტვირთვა უსაფრთხოა, დახურე და შეისწავლე საიტი მასზე დაბრუნებამდე. ყოველთვის სიფრთხილე გმართებს, როდესაც უცნობ საიტებს სტუმრობ.

- შეეკითხე მეგობრებს, თუ რამდენად სანდოა ეს საიტი, თუ აქვთ რაიმე გამოცდილება მასთან დაკავშირებით.

- მოიძიე ინფორმაცია საიტის შესახებ. გამოიყენე საძიებო სისტემა, რომ იპოვნო სიახლეები საიტის მფლობელი ორგანიზაციის შესახებ, ან მოიძიე ფორუმზე, თუ რას წერენ სხვა ადამიანები ამ საიტთან დაკავშირებით.

- შეამოწმე მისამართის ზოლი შენს ბრაუზერში. ზოგიერთი ზიანის მომტანი ვებგვერდი შექმნილია სხვა ცნობილი საიტების მსგავსად და მისამართების ზოლი ზუსტად გიჩვენებს რომელ საიტზე ხარ რეალურად.

- გამოიყენე Google safe browsing diagnostic „გუგლის საიტების უსაფრთხოების დიაგნოსტიკა“. დააკოპირე საიტის URL, ჩასვი დიაგნოსტიკის გვერდზე არსებულ ველში და დააჭირე ძებნის ღილაკს.

შენი ინფორმაცია ბრაუზერში

ყოველთვის, როცა ინტერნეტს იყენებ, იქმნება შენ მიერ მონახულებული საიტების სია, ასევე იწერება ყოველი დაკლიკვა. ამ ინფორმაციაზე დასაკვირვებლად ბევრი ვებ – გვერდი ბრაუზერში ინახავს მონაცემთა მცირე ფრაგმენტს სპეციალურ ფაილებში, რომლებიც cookie-ს სახელითაა ცნობილი.

ამის გარდა ვებსაიტმა ინტერნეტ აქტივობაზე დასაკვირვებლად შეიძლება გამოიყენოს მომხმარებლის პროფილი. იმის მიუხედავად, რომ ასეთი თვალთვალი შენს ონლაინ უსაფრთხოებას რისკის ქვეშ არ აყენებს, მნიშვნელოვანია იცოდე, როგორ ხდება შენს ონლაინ მონაცემებზე თვალყურის დევნება და გამოყენება.

რატომ აკვირდებიან ვებ საიტები ონლაინ აქტივობას?

მრავალი მიზეზი არსებობს იმისა, თუ რატომ შეიძლება აკვირდებოდეს ვებსაიტი შენს აქტივობას ინტერნეტში. ზოგიერთ შემთხვევაში ეს ინფორმაცია საჭიროა იმისათვის, რომ ინტერნეტში მუშაობის პროცესი უფრო სწრაფი და მოსახერხებელი გახადონ. მაგრამ ეს მონაცემები ასევე შეიძლება გამოიყენონ შენი ჩვევების და პრეფერენციების დასადგენად, ამ გზით რეკლამის გამავრცელებლები განსაზღვრავენ თუ რა რეკლამა გიჩვენონ ინტერნეტ სივრცეში.

შენი ინფორმაცია ბრაუზერში

ქვემოთ გიჩვენებთ, თუ როგორ აკვირდებიან ვებსაიტები შენს ონლაინ აქტივობას.

- ვიდეო საიტები, როგორებიცაა YouTube და Netflix, შენს მიერ ნანახი ვიდეოების შესახებ აგროვებენ ინფორმაციას, რომლის დახმარებითაც უფრო მეტ ისეთ ვიდეოს გთავაზობენ, რომლებიც შეიძლება მოგეწონოს.

- ინტერნეტ მაღაზიები Amazon და eBay, აწარმოებენ შენს მიერ ნანახი და შეძენილი საქონლის აღრიცხვას, რათა მომავალში შემოგთავაზონ სხვა პროდუქტები, რომელთა ყიდვაც შეიძლება მოისურვო მომავალში.

- ისეთი საძიებო სისტემა, როგორიც არის Google, აღრიცხავს თუ რას ეძებდი და რა ენაზე. ასე ის შენთვის უფრო შესაბამისი შემოთავაზების გაკეთებას ცდილობს, მაგრამ შესაძლებელია ზემოაღნიშნული რეკლამისთვისაც გამოიყენოს.

შენი ინფორმაცია ბრაუზერში

როგორ მუშაობს cookies?

Cookies-ს შეუძლია შეინახოს კონკრეტული ინფორმაცია თუ რომელ საიტებზე შედიხარ და რას აკლიკებ იქ. თუ რომელიმე საიტზე გაქვს პროფილი, ეს ინფორმაცია შენი ბრაუზერის Cookies -ს ფაილებში ინახება.

მაგალითად: ახალი ამბების საიტმა შეიძლება გამოიყენოს cookies, რომ შეამოწმოს ადრე შესულხარ ამ საიტზე, თუ არა და რა სტატიები წაიკითხე ბოლო ვიზიტისას, ამგვარად მას შეუძლია მსგავსი სტატიების შემოთავაზება შენ მიერ ადრე გაკეთებული არჩევანის მიხედვით.

შენი ინფორმაცია ბრაუზერში

უქმნიან თუ არა რისკს ჩემს კომპიუტერს Cookies ფაილები?

ზოგადად, Cookies – ფაილები შენი ონლაინ უსაფრთხოებისთვის საფრთხეს არ წარმოადგენენ - ნაკლებად სავარაუდოა, რომ მათი გამოყენებით მავნე პროგრამების მიღება შეძლო ან გააზიარო ფინანსური ინფორმაცია.

და, თუ მაინც არ მოგწონს ამ გზით შენ შესახებ ინფორმაციის შეგროვება, ბრაუზერში არსებობს Cookies – ს შეზღუდვის და კონტროლის პარამეტრები.

როგორ ავიცილოთ თავიდან Cookies ფაილების თვალთვალი

არსებობს Cookies მიერ ფაილების კონტროლის გათიშვის რამდენიმე გზა. ზოგიერთი საიტი თვითონ გაძლევს Cookies ფაილების გამორთვის შესაძლებლობას, თუმცა ამან შეიძლება გათიშოს საიტის ზოგიერთი ფუნქცია.

თუ დაგჭირდება, Cookies სრულად გათიშვა, სცადე ბრაუზერში „Do Not Track“ ფუნქციის ჩართვა. ბრაუზერების უმეტესობა ამ ფუნქციას ავტომატურად თიშავს, მისი გააქტიურება შესაძლებელია პრივატულობის პარამეტრებიდან (Privacy and security).

შენი ინფორმაცია ბრაუზერში

პროფილის თვალთვალი

მაშინაც კი, თუ ვებსაიტებს გაუთიშავ cookies ფაილების შენახვის ფუნქციას, არსებობს შენი შენს ჩვევებზე დაკვირვების სხვა გზებიც. მაგალითად, როდესაც პროფილს ქმნი ისეთ საიტზე, როგორიცაა Facebook ან Google, უფლებას აძლევ მათ შეისწავლონ და შეინახონ ინფორმაცია შენი აქტივობის შესახებ და ამ ინფორმაციას cookies ფაილში შენახვის ნაცვლად შეინახავს კომპანია.

ხშირ შემთხვევაში ეს ინფორმაცია შემდეგ მესამე მხარეს, რეკლამის განმთავსებლებს გადაეცემა, ინტერნეტით პერსონალიზებული რეკლამის მოსაწოდებლად. იმისდა მიუხედავად, გამორთავ, თუ არა ამ პარამეტრს ის მაინც ავტომატურად იქნება ჩართული.

დამატებითი უსაფრთხოება ტელეფონის გამოყენებით

ტელეფონით ვერიფიკაციის გამოყენება

თუ ბოლო რამდენიმე წლის მანძილზე გამოგიყენებია ელექტრონული ფოსტის სერვისი, როგორიცაა Gmail, Outlook.com, ან Yahoo, სავარაუდოდ მოგთხოვდნენ ტელეფონის ნომრის მითითებას შენი პროფილის დადასტურებისთვის.

რაც უფრო მეტ ყოველდღიურ ამოცანას ვასრულებთ ინტერნეტით, როგორიცაა გადასახადების გადახდა, ონლაინ მაღაზიებში შოპინგი, ვებპროვაიდერებისთვის უფრო მეტად საჭირო ხდება შენი იდენტობის შემოწმება, რომ არ დაუშვან მისი უკანონო გამოყენება. ტელეფონის ნომერი ერთ-ერთი უმარტივესი საშუალებაა შენი იდენტობის დასადასტურებლად.

დამატებითი უსაფრთხოება ტელეფონის გამოყენებით

როგორ მუშაობს ტელეფონით ვერიფიკაცია?

როცა პროფილს ქმნი ან პაროლის აღდგენას ცდილობ, პროვაიდერი მოგთხოვს ტელეფონის ნომრის შეყვანას. შემდეგ პროვაიდერი გამოგიგზავნის შეტყობინებას ან დაგირეკავს ტელეფონზე და შეგატყობინებს დადასტურების კოდს, რომლის შეყვანაც შემდეგ შეგიძლია საიტზე. ამ გზით ისინი ადგენენ, რომ ეს შენ ხარ და არა სხვა ვიღაც, ვინც შენს პროფილში შეღწევას ცდილობს.

უქმნის თუ არა საფრთხეს ტელეფონით ვერიფიკაცია ჩემს უსაფრთხოებას?

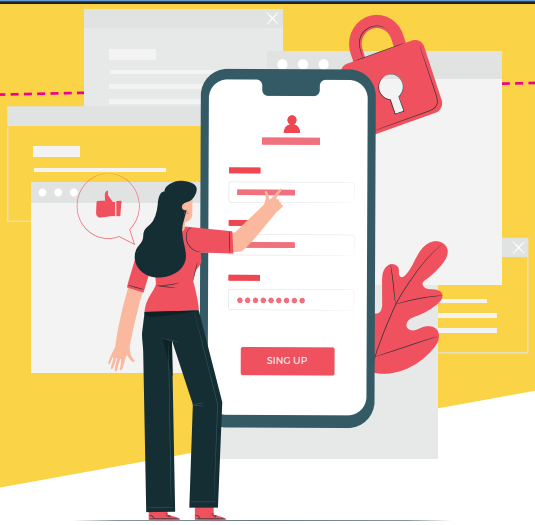
ყველა არ გრძნობს თავს კომფორტულად, როდესაც საკუთარ ნომერს Google და Microsoft-ის მსგავს მსხვილ კომპანიებს უზიარებს. მაგრამ მიუხედავად იმისა, რომ გეჩვენება ბევრი პირადი ინფორმაცია გაეცი, მნიშვნელოვანია გესმოდეს, რომ ეს შენი ანგარიშის დასაცავად კეთდება.

დამატებითი უსაფრთხოება ტელეფონის გამოყენებით

ტელეფონით ვერიფიკაციისას შენ პროვაიდერს უზუნველყოფ საგანგებო საკონტაქტო ნომრით - თუ წარმოიქმნება პროფილთან დაკავშირებული პრობლემა, სერვისის მომწოდებელი უშუალოდ დაგიკავშირდება.

ზოგიერთი სერვისი, როგორიცაა Google და Facebook, საშუალებას გაძლევს გამოიყენო ტელეფონის ნომერი ორ საფეხურიანი ვერიფიკაციის პროგრამაში.

ტელეფონის გამოყენება დაგჭირდება, როდესაც პროფილში უცხო მოწყობილობიდან შედიხარ, ამ დროს პროვაიდერი გთხოვს დასტურის კოდის შეყვანას. ეს გაცილებით ურთულებს ჰაკერს შენი პროფილის გატეხვას.



სოციალურ ქსელებში ქცევის წესები

ქსელში მოგზაურობა შეიძლება ერთდროულად კარგი გასართობიც იყოს, სასარგებლო საქმიანობაც, და ურთიერთობის საშუალებაც, როგორც უფროსებისთვის, ასევე ბავშვებისთვისაც. თუმცა ინტერნეტის ყველა მომხმარებელს უნდა ახსოვდეს, რომ ის მარტო არ არის ქსელში და როგორც რეალურ ცხოვრებაში, ასევე ქსელშიც არსებობს ქცევის წესები, რომელთა დაცვაც აუცილებელია.

ჩვენ ამ წესების ათვისებას გირჩევთ:

- მიმართე სხვებს ისე, როგორც ისურვებდი, რომ შენთვის მოემართათ.
- გახსოვდეს, რომ შენს შეტყობინებას ცოცხალი ადამიანი ღებულობს.
- მუდამ გახსოვდეს ონლაინ სივრცეში სათანადოდ მოქცევის წესები.
- აპატიე შეცდომები სხვებს, განსაკუთრებით ახალბედებს.
- ყოველთვის შეინარჩუნე სიმშვიდე, განსაკუთრებით მაშინ, თუ ვინმე შენთვის შეურაცხყოფის მოყენებას ცდილობს, იგნორირება გაუკეთე მას.
- ეცადე არ დაწერო ტექსტი დიდი ასოებით, მისი მნიშვნელობის გასაძლიერებლად, ზოგიერთი მომხმარებლის აზრით ეს ყვირილთან ასოცირდება.

სოციალურ ქსელებში ქცევის წესები

- არ გამოიყენო შეუსაბამო ან შეურაცხმყოფელი ლექსიკა.
- გამოიყენე მუდმივი ონლაინ სახელი ან ფსევდონიმი. კარგად დაფიქრდი, ელ.ფოსტის მისამართის ან პროფილის სახელის შექმნამდე. ორივე შემთხვევაში შეგიძლია ასოების და ციფრების კომბინაციის გამოყენება.
- არასოდეს გააგზავნო და გაავრცელო არასასურველი შეტყობინებები, ჩვეულებრივ ამას სპამს ეძახიან.
- თავი შორს დაიჭირე გაჭიანურებული ემოციური კამათისგან და „შეიმისგან“.
- ფრთხილად შეარჩიე ონლაინ მეგობრები. ზოგიერთი საიტი უამრავი მეგობრის დამატების საშუალებას იძლევა. ზოგჯერ ბავშვები ეჯიბრებიან კიდეც ერთმანეთს, თუ რომელი მოაგროვებს უფრო მეტ მეგობარს. მაგრამ ონლაინ მეგობრები იგივე არ არის, რაც რეალური მეგობრები.
- შეამოწმე დაწერილი ტექსტის სისწორე, ნათლად და ლაკონურად ჩამოაყალიბე სათქმელი.
- მოიქეცი სათანადოდ, ზუსტად ისევე, როგორც რეალურ ცხოვრებაში.

ტექნოლოგიებისგან დასვენება

გვიან ღამით შეტყობინებების მიღებამ და გაგზავნამ შეიძლება ძილთან დაკავშირებული პრობლემები გამოიწვიოს. ღამის ზარებმა და ვიბრაციამ შეიძლება ძილი დაგირღვიოს, სკოლაში წასვლის წინ კი დაღლილობა იგრძნო. ძილის უკმარისობამ ან შეწყვეტილმა ძილმა შეიძლება ყველაფერზე იქონიოს გავლენა დაწყებული შენი განწყობიდან სპორტული შედეგებით დამთავრებული.

როგორ იყო მიუწვდომელი ძილის დროს?

აქ მოცემულია რამდენიმე რჩევა, რომლებიც დაგეხმარება ენერგიით დამუხტვაში და დილით კონცენტრაციის გაძლიერებაში.

1. ჩახურე მესენჯერის ტიპის ყველა აპლიკაცია, სოციალური მედია და ელ.ფოსტა. შემოსული შეტყობინების ხმამ შეიძლება ძილი დაგიფრთხოს, იმ შემთხვევაშიც თუ ადგომას და მათზე პასუხის გაცემას არ აპირებ სავარაუდოდ, შენი მეგობრებიც გავლენ ქსელიდან როცა ნახავენ, რომ შენც გასული ხარ.

2. ძილის წინ გამორთე მობილური ტელეფონი (არ გადაიყვანო ის ვიბრაციის რეჟიმზე). ღამით ვიბრაციის ხმა ისეთივე ხმამაღალი იქნება, როგორც შემოსული ზარის ხმა.

ტექნოლოგიებისგან დასვენება

3 ჩვევად აქციე ძილის წინ ყველა ელექტრო მოწყობილობის გამორთვა, განსაკუთრებით, თუ ისინი შენს ოთახში არიან. დაძინებამდე 2 საათით ადრე გათიშე ყველა ელექტრო მოწყობილობა: ლეპტოპი, ტაბლეტი, ტელევიზორი და ვიდეო კონსოლები.

4 ღამით ოთახიდან გაიტანე ტელეფონი და პლანშეტი, უმჯობესია სხვა ოთახში დამუხტო ისინი. სანამ ელემენტი იმუხტება გამოძინებას მოახერხებ.

5 კარგად გამოიძინე, რომ კარგად გამოიყურებოდე და თავსაც კარგად გრძნობდე. ძილი საუკეთესო საშუალებაა იმისათვის, რომ დილით თავი დასვენებულად იგრძნო და ასევე გამოიყურებოდე. იმისათვის, რომ კარგად გამოძინება მოასწრო, წინასწარ უთხარი შენს მეგობრებს როდის შეწყვეტ მოკლედ ტექსტურ შეტყობინებებსა და ზარებზე პასუხის გაცემას. ასე მათ ეცოდინებათ, რომ შეტყობინებებმა უნდა დაიცადონ. ეცადე გამოეთიშო ყველაფერს დაძინებამდე 2 საათით ადრე.

6 შეიძლება ძალიან რთულად მოგეჩვენოს ღამით ტექნიკის გამორთვა. მაგრამ შენი მოწყობილობებისთვის კომენდანტის საათის დაწესება გაგიადვილებს დაძინებას და შენს ტვინს მისცემს ტექნიკისგან დასვენების საშუალებას.

ინტერნეტის გამოყენება შენს სასარგებლოდ

ინტერნეტი ინფორმაციის უძირო წყაროა, რომელიც მუდამ ხელთ გვაქვს, რა თქმა უნდა თუ მისი სწორად გამოყენება იცი. რაღაც შეიძლება ენციკლოპედიიდან ან წიგნებიდან გაიგო, რაღაც მშობლებს ან ნაცნობებს შეეკითხო, მაგრამ რამდენი დრო შეიძლება დაიხარჯოს პასუხის ძიებაში? ინტერნეტი ინფორმაციის მიღების ყველაზე უსწრაფესი გზაა. ხოლო საჭირო ინფორმაციის ძებნის ცოდნა - ეს ღირებული თვისებაა, რომელიც მომავალში სასარგებლო იქნება შენთვის.

ინტერნეტი ასევე ყურადღების და მეხსიერების ვარჯიშის შესაძლებლობაა. აზროვნების პროცესის განვითარება ხშირად, ლოგიკური ამოცანების ამოხსნით და თამაშების დახმარებით ხდება. მთავარია ეკრანთან გატარებული დროის დოზირება და ასაკის შესაბამისი თამაშების შერჩევა.

თამაშის საშუალებით უფრო სწრაფად ეცნობი სამყაროს, კომპიუტერული საგანმანათლებლო თამაშების დახმარებით შეგიძლია მიიღო ბევრი სასარგებლო ინფორმაცია და გაიფართოვო ჰორიზონტები. სპეციალურ საიტებზე შეგიძლია მსოფლიოს სხვადასხვა კუთხის პანორამების ნახვა, მუზეუმების მონახულება, ცხოველთა სამყაროს სხვადასხვა წარმომადგენლების დათვალიერება.

ინტერნეტის გამოყენება შენს სასარგებლოდ

ინტერნეტი ასევე შესანიშნავი დამხმარეა უცხო ენების სწავლის საქმეში. ინტერნეტით შეგიძლია უცხო ენის არა მხოლოდ საგანმანათლებლო პროგრამების და თამაშების შერჩევა, არამედ სიმღერების, მულტფილმების, პროგრამების. უფრო მეტიც, შეგიძლია კომუნიკაცია ამ ენის მატარებელ ხალხთან ან თუნდაც საინტერესო ონლაინ კურსების გავლა.

გარდა ამისა ინტერნეტი დიდ მანძილზე კომუნიკაციის შესაძლებლობას იძლევა. ჩვენ შეგვიძლია ყოველდღე დავუკავშირდეთ ჩვენს ოჯახს და მეგობრებს, როდესაც ისინი რაიმე მიზეზით სხვაგან იმყოფებიან. ინტერნეტის გამოგონებამდე საჭირო იყო ლოდინი, სანამ ადრესატი წერილს მიიღებდა, ასევე უნდა გეცადა პასუხისთვის, მაგრამ დღეს შეგიძლია ნებისმიერ კონტინენტზე დარეკვა დღის ნებისმიერ დროს და გარდა ამისა შეგიძლია უყურო შენს თანამოსაუბრეს.

ინტერნეტის გამოყენება შენს სასარგებლოდ

ონლაინში ძიების გამარტივების ხუთი გზა

როდესაც სტატიას წერ ან პროექტს აკეთებ, ინტერნეტში შესვლა კვლევების ჩასატარებლად სირთულეს არ წარმოადგენს. მაგრამ ყველა ხელმისაწვდომი შედეგი შეიძლება არადამაჯერებლად მოგეჩვენოს. იმის ცოდნა, თუ როგორ შეარჩიო და შეაფასო ონლაინ რესურსი ბევრ თავის ტკივილს და დროის ფუჭად ხარჯვას აგაცილებს თავიდან.

როგორ უნდა გახადო ინტერნეტში ძებნა მაქსიმალურად მარტივი და ეფექტური:

- დაიწყე სკოლიდან. შეეკითხე მასწავლებელს ან ბიბლიოთეკარს, თუ რომელ წყაროებს გირჩევდნენ შენი პროექტისთვის. ამ გზით შეგიძლია დარწმუნდე, რომ ეს რესურსები დამტკიცებულია სკოლის მიერ და იქ განთავსებული ინფორმაცია ზუსტია. ზოგჯერ მასწავლებელს ან სკოლას გამოწერილი აქვს ფასიანი ონლაინ ჟურნალები ან ვებ გვერდები და მათ ისეთი ინფორმაციის მოცემა შეუძლიათ, რასაც ინტერნეტში უბრალო ძიებით ვერ ნახავ. თუ შენი მასწავლებელიც ასე ფიქრობს, ინტერნეტი გამოიყენე, როგორც ინფორმაციის დამატებითი წყარო, ხოლო ინფორმაციის ძიების პირველად წყაროდ შეგიძლია სასკოლო ბიბლიოთეკის, წიგნებისა და ჟურნალების გამოყენება.

ინტერნეტის გამოყენება შენს სასარგებლოდ

განაცალკევე ფაქტი ფიქციისგან. ვიდრე კვლევას დაიწყებდე გააკეთე შენს თემასთან დაკავშირებული საიტების ჩამონათვალი, შეამოწმე რამდენად სანდო და აქტუალურია საიტი, მითითებულია თუ არა ავტორი და წყაროები. სამთავრობო ვებ გვერდები ბოლოვდება gov-ით, საგანმანათლებლო საიტები edu-ით, ძირითადად მათზე განთავსებული ინფორმაცია სწორია. საინფორმაციო საიტებიც შეიძლება გამოგადგეს, მაგრამ დარწმუნდი, რომ პირველწყაროს იყენებ. თუ სტატიაში სხვა წყაროა მითითებული, მაგალითად ორგანიზაცია ან ვებგვერდი, გადადი უშუალოდ ამ წყაროზე. org -ით დაბოლოვებული საიტები ძირითადად არაკომერციულ ორგანიზაციებს ეკუთვნის.

ეს საიტებიც შეიძლება კარგ წყაროდ ჩაითვალოს, მაგრამ გადაამოწმე მასწავლებელთან თუ მიიჩნევს მათ ასეთად. Wikipedia.org პოპულარულია, მაგრამ ამ გვერდზე ყველას შეუძლია ცვლილებების შეტანა, ამიტომ სკოლების უმეტესობა მას სანდო წყაროდ არ მიიჩნევს. კომერციული საიტები ბოლოვდება com -ით, ისინი ძირითადად პროდუქციის გაყიდვაზე არიან ორიენტირებულნი. ბლოგები და პირადი გვერდები, როგორიცაა YouTube, Digg, Tumblr, Pinterest, ან Facebook ფაქტებთან ერთად ხშირად სუბიექტურ ინფორმაციასაც იძლევიან.

ინტერნეტის გამოყენება შენს სასარგებლოდ

- **იყავი კონცენტრირებული.** როდესაც თემაზე მუშაობ გამორთე სოციალური მედია და ტელეფონი. თუ შესვენების გაკეთება დაგჭირდება ჩაინიშნე სად გაჩერდი. ყოველ ერთ საათში 5-10 წუთიანი შესვენებების გაკეთება საკმარისია.

- **გააკეთე სწორი ციტირებები.** როდესაც ტექსტის გადმოტანა გჭირდება, არ დაგავიწყდეს წყაროს მითითება ან ამ ტექსტის საკუთარი სიტყვებით გადმოცემა. შემთხვევით პლაგიატიზმსაც შეიძლება სერიოზული შედეგები მოჰყვეს შენი ნაშრომის შეფასებისას.

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) - 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.

ლექსიკონი

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

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.

სპამი - წერილების გაგზავნა მიმღების თანხმობის გარეშე.

ლექსიკონი

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.

ფიშინგი - შეტყობინებები, რომლებიც ცდილობენ გამოგტყუონ მნიშვნელოვანი ან/და პირადი ინფორმაცია.

მავნე პროგრამა - პროგრამა რომელიც თავდამსხმელების მიერ გამოიყენება კომპიუტერის ფუნქციონირებისათვის ხელის შესაშლელად და პირად ინფორმაციასთან წვდომის მოსაპოვებლად. ის შეიძლება იყოს კოდი წარმოდგენილი სკრიფტის ან სხვა პროგრამის სახით.