საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

სასარგებლო რჩევები დისტანციურად მომუშავე თანამშრომლებისთვის

თბილისი

მარტი, 2020

მიმოხილვა

ახალი ტიპის Covid-19 კორონავირუსის გავრცელების საშიშროების გამო, არაერთმა ორგანიზაციამ თანამშრომლები დისტანციური მუშაობის რეჟიმზე გადაიყვანა. ორგანიზაციები ამ გზით ცდილობენ მოუფრთხილდნენ და დაიცვან თავიანთი თანამშრომლების ჯანმრთელობა. დისტანციური მუშაობის რეჟიმში ორგანიზაციები ცდილობენ შეინარჩუნონ პროდუქტიულობის ბალანსი, თუმცა არ უნდა დაგვავიწყდეს, რომ ონლაინ რეჟიმში მუშაობით კიბერრისკებიც იზრდება. ბევრი კომპანიისთვის დისტანციურად მუშაობა ახალი გამოწვევაა, შეაბამისად კიბერრისკების გათვალისწინების ნაკლები გამოცდილება აქვთ.

წარმოგიდგენთ გზამკვლევს, რომლის დახმარებითაც თქვენი დისტანციური მუშაობის პროცესი უფრო უსაფრთხო გახდება.

რისკები

ჩვენ მოვახდინეთ 3 ძირითადი საფრთხის იდენტიფიცირება, რომელიც თან ახლავს დისტანციურ მუშაობს. თითოეულ მათგანთან დაკავშირებით წარმოგიდგენთ შესაბამის ინფორმაციას და დამატებით საკითხავ მასალას, დანართების სახით.

სოციალური ინჟინერია

ერთ-ერთი ყველაზე დიდი საფრთხე, რომლის წინაშე დისტანციურად მომუშავე ადამიანი ხვდება, არის სოციალური ინჟინერია. სოციალური ინჟინერია ჰაკინგის ერთ-ერთი ყველაზე ფართოდ გავრცელებული მეთოდია. ის დამყარებულია ინდივიდის ფსიქოლოგიურ მანიპულაციაზე, როდესაც მსხვერპლს არწმუნებენ შეასრულოს კონკრეტული ქმედებები ან გაახმაუროს კონფიდენციალური ინფორმაცია. კიბერკრიმინალები იყენებენ ტყუილს, ქრთამს ან შიშის ფაქტორს, რათა შეაღწიონ თქვენს ინფორმაციულ სისტემებში. ყველაზე ხშირად ინტერნეტ-თაღლითობისთვის კიბერკრიმინალები მიმართავენ ფიშინგს. ფიშინგი ინტერნეტ თაღლითობის ფორმაა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პერსონალური მონაცემები (პირადი საიდენტიფიკაციო მონაცემები, პაროლი, საკრედიტო ბარათის და საბანკო ანგარიშის ნომერი ან სხვა კონფიდენციალური ინფორმაცია).

ფიშინგის მსხვერპლი ძირითადად უყურადღებო მომხმარებელი ხდება, რომელიც არასანდო წყაროს (ერთი შეხედვით ნაცნობ ვებ-გვერდს წააგავს) გაანდობს პირად ინფორმაციას. ამიტომ, ფიშინგ-შეტევებისგან თავდაცვის მიზნით:

- არ გამოიყენოთ სამსახურებრივი ელ-ფოსტა პირადი ანგარიშებისა და აქტივობებისთვის;
- დააკვირდით წერილის ადრესატს;
- გამოიჩინეთ სიფრთხილე მიმაგრებული ფაილების მიმართ;
- კარგად დაფიქრდით ბმულზე გადასვლამდე;
- დარწმუნდით ვებ-გვერდის უსაფრთხოებაში;

- არასოდეს ჩამოტვირთოთ ფაილები საეჭვო ვებ-გვერდებიდან;
- არასოდეს გასცეთ პერსონალური ინფორმაცია ელ-მიმოწერით.

დამეტებითი ინფორმაციისთვის იხილეთ დანართი 1.

პაროლები

გამოიყენეთ რთული პაროლი. მარტივი პაროლის შემთხვევაში კიბერკრიმინალები ადვილად შეძლებენ მის გატეხვას და განახორციელებენ არაავტორიზებულ წვდომას თქვენს მონაცემებზე. პაროლი უნდა შედგებოდეს:

მინიმუმ 8 სიმბოლოს, მაღალი და დაბალი რეგისტრის ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს (მაგალითად: !@#$%^&*()_+).

პაროლის შესაქმნელად არ გამოიყენოთ ისეთი სახის ინფორმაცია, როგორიცაა, მაგალითად: სიტყვები ლექსიკონიდან, სახელები, დაბადების დღეების თარიღები და სხვა.

არ გამოიყენოთ ერთი და იგივე პაროლი. კიბერკრიმინალის მიერ პაროლის მოპოვების შემთხვევაში, საფრთხის ქვეშ დადგება ყველა ის რესურსი, რომელზეც ეს პაროლი გიყენიათ. სხვადასხვა პაროლის შემთხვევაში თქვენ ახდენთ რისკების და შესაძლო დანაკარგების მინიმიზაციას.

გამოიყენეთ პაროლების მენეჯერი. პაროლების მენეჯერის დახმარებით შესაძლებელია დაიმახსოვროთ მხოლოდ ერთი მთავარი პაროლი. ყველა სხვა პაროლი დაიშიფრება მენეჯერის მიერ. ამ გზით თქვენი ორგანიზაციის გუნდის წევრთა პაროლებსაც დავიცავთ. ეს პაროლების გაზიარების საშუალებასაც გვაძლევს, რაც ნიშნავს, რომ თითოეული პირი შესძლებს სისტემაში ავტორიზებას პაროლის უნებურად გამჟღავნების გარეშე.

გამოიყენეთ ორმაგი ავტენთიფიკაციის ფუნქცია, რომლის დროსაც ავტორიზაციისთვის სახელის და პაროლის შეყვანა არ არის საკმარისი, სისტემა მოითხოვს დამატებითი ეტაპების გავლას, როგორიცაა მაგალითად მობილურ ტელეფონზე ან ელ ფოსტაზე მიღებული ერთჯერადი კოდი.

დამატებითი ინფორმაციისთვის იხილეთ დანართი 2.

განახლებული ოპერაციული სისტემა და პროგრამული უზრუნველყოფა

მესამე ძირითად რისკს წარმოადგენს ოპერაციული სისტემისა და პროგრამული უზრუნველყოფის განახლების საკითხი. მნიშვნელოვანია, რომ თქვენი ნებისმიერი მოწყობილობა, რომელსაც სამსახურებრივი მოვალეობის შესრულებისთვის იყენებთ, იყოს პროგრამულად განახლებული.

საყურადღებო საკითხები

რჩევები სახლში უსაფრთხო კიბერგარემოს შესაქმნელად

იხ.დანართი 3

უკაბელო ქსელი (Wi-Fi)

იხ.დანართი 3

ბავშვების დაცვა ინტერნეტ-სივრცეში

იხ.დანართი 4

უსაფრთხოების რეკომენდაციები

სახლიდან მუშაობისას გადამწყვეტი მნიშვნელობა აქვს თანამშრომლების კომპიუტერების უსაფრთხოებას. თქვენი ელექტრონული მოწყობილობის დაინფიცირებით შესაძლოა მთელი კორპორატიული ქსელის კომპრომეტირება მოხდეს. გაითვალისწინეთ შემდეგი რჩევები:

- დაბლოკილ მდგომარეობაში დატოვეთ თქვენი ელექტრონული მოწყობილობების ეკრანი.
- არ შეაერთოთ უცხო ელექტრონული მედია მატარებელი კომპიუტერზე.
- შექმენით კომპიუტერში არსებული ინფორმაციის სარეზერვო ასლები.
- დაშიფრეთ მნიშვნელოვანი მონაცემები და ფაილები.
- გამოიყენეთ პროგრამა „find my device". (ელექტრონული მოწყობილობის დაკარგვის შემთხვევაში, მისი პოვნა ამ აპლიკაციით გაგიადვილდებათ).

რა არის PGP და როგორ მუშაობს ის?

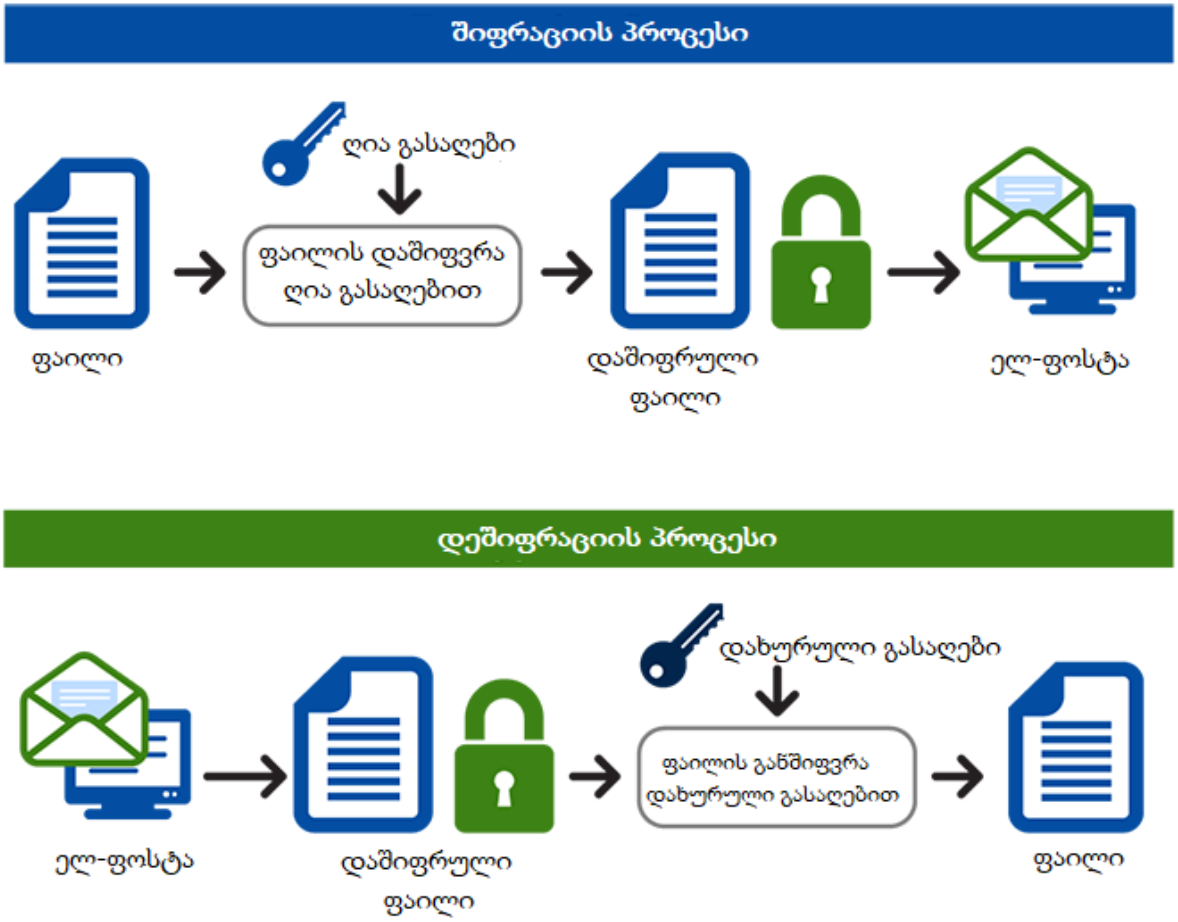
რა არის PGP?

PGP (Pretty Good Privacy) დაშიფრვა ინტერნეტ-უსაფრთხოების ერთ-ერთი ძირითად საყრდენს წარმოადგენს, ვინაიდან ის მომხმარებლებს შესაძლებლობას აძლევს უზრუნველყოს გაგზავნილი ფაილების უსაფრთხოება.

PGP შეიქმნა 1991 წელს პროგრამული უზრუნველყოფის ინჟინერის ფილ ციმერმანის მიერ, რომელმაც ეს ტექნოლოგია გამოიყენა გლობალურ ქსელში, ინფორმაციის უსაფრთხოდ მიმოცვლისთვის.

დღეს-ღეობით PGP-ს ფლობს კომპანია სიმანტეკი. თუმცა, ელ-ფოსტის შიფრაციის სტანდარტი OpenPGP ჩაშენებულია რამდენიმე პროგრამულ უზრუნველყოფაში.

როგორ მუშაობს PGP?



ელ-ფოსტა არ არის კომუნიკაციის ყველაზე დაცული საშუალება. როდესაც ელექტრონული წერილი სცდება თქვენს ანგარიშს, ის ხვდება გლობალურ ქსელში და სცდება თქვენი კონტროლის ფარგლებს.

მაშინ, როდესაც გსურთ მნიშვნელოვანი და სენსიტიური ინფორმაციის გადზავნა, ელ-ფოსტის გამოყენება არ არის საუკეთესო გადაწყვეტილება. შესაძლოა, წერილი აღმოჩნდეს ჰაკერების ხელში და ბოროტმოქმედებმა მოიპარონ თქვენი კონფიდენციალური ინფორმაცია.

სწორედ ეს საფრთხე დაედო საფუძვლად PGP-ს შექმნას, რომლის წყალობითაც ხდება ინფორმაციის დაშიფვრა და განშიფვრა მხოლოდ ავტორიზებული პირების მიერ, შესაბამისი, განსხვავებული გასაღებებით. აღნიშნული იძლევა საშუალებას, რომ, ტექნოლოგიის სწორად გამოყენების შემთხვევაში, ინფორმაციის კონფიდენციალობა, სისრულე და ხელმისაწვდომობა იყოს მაქსიმალურად დაცული.

ერთ მხარეს, რომელიც აზიარებს ფაილს, აქვს ღია გასაღები (რომელიც შიფრავს შეტყობინებას), ხოლო, მეორე მხარეს აქვს დახურული გასაღები (რომელიც ახდენს შეტყობინების დეშიფრაციას (განშიფვრას).

OpenPGP

1997 წელს PGP ტექნოლოგიის საფუძველზე შეიმუშავეს უსაფრთხოების სტანდარტი, რომელსაც დაარქვეს OpenPGP.

OpenPGP დღეს-დღეობით წარმოადგენს ელ-ფოსტის შიფრაციის გავრცელებულ სტანდარტს.

სხვა საკითხავი მასალა

წარმოგიდგენთ დამატებით საკითხავ მასალას კომპიუტერული უსაფრთხოების უზრუნველყოფის შესახებ.

ზოგადი რჩევები

თავდაცვა რეალური კიბერსაფრთხეებისგან

იხ.დანართი 5

უსაფრთხოების ზომები, რომელიც კომპიუტერის ინტერნეტთან დაკავშირებამდე უნდა გავითვალისწინოთ

იხ.დანარი 6

USB უსაფრთხოება

იხ.დანართი 7

ვებ-ბრაუზერის უსაფრთხოება

იხ.დანართი 8

სმარტფონის უსაფრთხოება

იხ.დანართი 9

სოციალური ქსელი

იხ.დანართი 10

ინფორმაციის ონლაინ განთავსების რეკომენდაციები

იხ.დანართი 11

რამდენად ანონიმურები ვართ ინტერნეტ-სივრცეში

იხ.დანართი 12

სოციალური ინჟინერია

ელ.ფოსტაზე მიმაგრებული ფაილებისგან თავის დაცვის წესები

იხ.დანართი 13

სპამ წერილები

იხ.დანართი 14

დამატებითი

თავდაცვა ვირუსებისა და ჭიებისგან

იხ.დანართი 15

შანტაჟის/გამოსასყიდი პროგრამული უზრუნველყოფა

იხ.დანართი 16

ჯაშუში პროგრამა

იხ.დანართი 17

დანართები

დანართი 1

ფიშინგი

ფიშინგი არის ელექტრონული ფოსტის მისამართისა ან ყალბი ვებ გვერდის გამოყენებით განხორციელებული თავდასხმა. თავდასხმის მიზანს წარმოადგენს პერსონალური, სამსახურეობრივი და ფინანსური ინფორმაციის მოპარვა. მსხვერპლი იღებს ყალბ წერილს, რომელიც ვითომ გამოგზავნილია ლეგიტიმური წყაროდან (თანამშრომელი, სერვის პროვაიდერი, ბანკი, შესაბამისი კომპანია ან ორგანიზაცია), რომელთანაც მომხმარებელს აქვს შეხება, სადაც რაიმე მიზეზით სთხოვენ გაანახლოს თავისი მონაცემები მითითებული ბმულის საშუალებით, გახსნას წერილზე მიმაგრებული ფაილი ან შეიძლება მოცემული იყოს შესასრულებლად სხვადასხვა ტიპის ინტრუქცია. წერილის ადრესატი შეიძლება ასევე ითხოვდეს ისეთი ტიპის პერსონალურ ინფორმაციას როგორიცაა პაროლები, პერსონალური მონაცემები, საიდენტიფიკაციო ნომრები და ა.შ. მოთხოვნილი ინფორმაციის მიღების შემდეგ თავდამსხმელები მოიპოვებენ სრულ კონტროლს მსხვერპლთა ანგარიშებზე.

ფიშინგ წერილების დამახასიათებელი ნიშანია მაღალი ხარისხის გაყალბება. სავაჭრო ფედერალურ კომისიას წარმოდგენილი აქვს მაგალითები თუ როგორი შინაარსის შეიძლება იყოს ფიშინგ წერილები:

- თქვენ შეგიჩერდებათ მომხმარებლის ანგარიში, თუ არ მოხდება პაროლის ან საკრედიტო ბარათის ინფორმაციის განახლება მოცემულ ვებ გევრდზე.
- თქვენს ანგარიშზე მოხდა არა ავტორიზებული შეღწევა, გთხოვთ გადახვიდეთ ბმულზე რათა დაადასტუროთ თქვენი იდენტობა
- თქვენი ანგარიშიდან მოხდა თანხის ჩამოჭრა. გთხოვთ დაგვიკავშირდეთ 7 დღის განმავლობაში რათა თანხა აგინაზღაურდეთ.

თუ თვლით რომ მიიღეთ ფიშინგ წერილი, გსურთ გადადგათ გარკვეული ნაბიჯები თავის დასაცავად და ასევე ნახოთ მსგავსი ტიპის წერილები, გთხოვთ ეწვიოთ ვებ გვერდს: https://www.irs.gov/privacy-disclosure/report-phishing

რჩევები უსაფრთხოებისთვის:

- თუ მიიღებთ მეილს, რომელიც გთხოვთ რომ გადახვიდეთ ვებ-ბმულზე ან გახსნათ მიმაგრებული დოკუმენტი, გადაამოწმეთ შეტყობინება. თუ მეილი წარმოჩენილია როგორც ნაცნობი ორგანიზაციისგან ან პირისგან გამოგზავნილი, გადაამოწმეთ შესაბამისი ორგანიზაციის ან პირის საკონტაქტო დეტალები, რომელიც თქვენთვის არის ცნობილი. დაუკავშირდით კომპანიას ოფიციალურ ნომერზე და დარწმუნდით რომ წერილი რეალური ადრესატისგან მიიღეთ.
- თავი აარიდეთ ისეთ კომუნიკაციას რომლის დროსაც გთხოვენ სასწრაფო/გადაუდებელ მოქმედებას.
- დაეჭვდით თუ წერილის შინაარსი დაუჯერებლად საინტერესოა.

- გამოიყენეთ ანტივირუსი და დარწმუნდით რომ თქვენი ანტივირუსის დროდადრო ახლდება.
- გამოიყენეთ გრძელი და რთული პაროლები, რომელიც შეიცავს ციფრებს, დიდ და პატარა ასოებს და რაიმე სიმბოლოს, რათა თავდამსხმელს გაუჭირდეს თქვენს ანგარიშში შეღწევა
- არ დააკლიკოთ ბმულს, დააკოპირეთ ის და ისე გადაიტანეთ მეილიდან ვებ-ბრაუზერში, მიიტანეთ მაუსი ბმულთან, სადაც გამოჩნდება ბმულის რეალური მისამართი
- გამოიყენეთ ორმაგი ავთენტიფიკაცია, განსაკუთრებით სენსიტიურ ანგარიშებზე როგორიცაა საბანკო ანგარიშები და პერსონალური ელექტრონული ფოსტის ანგარიშები. მომხმარებლის ანგარიშზე შესასვლელად, თქვენ მიიღებთ ერთჯერად კოდს მობილურ ტელეფონსა ან ელექტრონულ ფოსტაზე, ეს გაუმნელებს თავდამსხმელებს განახორციელონ შეტევა და თქვენი ანგარიშიც უფრო დაცული იქნება. ორმაგი ავთენტიფიკაციის საკითხთან დაკავშირებით დამატებითი ინფორმაციის მიღების სურვილის შემთხვევაში ეწვიეთ ლინკს: https://www.lockdownyourlogin.org/

დანართი 2

პაროლების უსაფრთხოება

ინტერნეტ სივრცეში მუდმივად ხდება კიბერშეტევები ვებ-გვერდებსა და სერვერებზე. თავდამსხმელები ცდილობენ ჩვენი პაროლების გამოცნობას და რაც უფრო მარტივი კომბინაციით შედგენილი პაროლი გვიყენია, მით უფრო დიდია შანსი იმისა, რომ კიბერშეტევის მსხვერპლნი გავხდეთ. საფრთხის თავიდან აცილება შეგვიძლია გრძელი 8-64 სიმბოლომდე შემდგარი პაროლის გამოყენებით და დაიმახსოვრეთ, სასურველია თქვენი პაროლი მხოლოდ თქვენ იცოდეთ.

რა დამატებითი ღონისძიებების განხორციელება გვესაჭიროება პაროლების უსაფრთხოებისთვის?

MFA, იგივე ორმაგი ავთენთიფიკაცია არის ფუნქცია, რომელიც გულისხმობს ელექტრონულ პლატფორმაზე პაროლის შეყვანის შემდგომ მომხმარებლის მიერ მიღებული ერთჯერადი კოდით იდენტობის დადასტურებას. ეს მეთოდი უკეთ ზღუდავს მომხმარებელთა რწმუნებებისა და მომხმარებლის რესურსების ხელმისაწვდომობას.

რა მექანიზმები გამოიყენება პაროლების დაცულობის ამაღლებისთვის?

დააყენეთ ანგარიშები ავტომატურ გაუქმებაზე - ანგარიშზე დიდი ხნის განმავლობაში არ შესვლის შემთხვევაში ანგარიში ავტომატურად გაუქმდება

გამოიყენეთ ანგარიშების ავტომატური დაბლოკვის მექანიზმი - პაროლის რამდენიმეჯერ არასწორად შეყვანის შემთხვევაში, თქვენი ანგარიში დაიბლოკება მცირე პერიოდით.

გამოიყენეთ ავთენტიფიკაციის ძლიერი მექანიზმები - ძლიერი პაროლები გიცავთ არაავტორიზებული პირებისგან, რომელთაც თქვენს ანგარიშზე წვდომის მოპოვება სურთ.

რა უნდა მოიმოქმედოთ თუ პაროლი დაკარგეთ ან დაგავიწყდათ?

შესაძლებელია მყარი დისკის დაფორმატების ან სხვა რაიმე მიზეზის გამო დავკარგოთ ან დაგვავიწყდეს პაროლები, რომელიც ავტომატურად იყო დამახსოვრებული. ამ ან სხვა მსგავსი შემთხვევის გამო მოყენებული ზიანის თავიდან ასაცილებლად ეცადეთ მნიშვნელოვანი ინფორმაციის სარეზერვო ასლები შექმნათ. თუმცა ზოგადად, ასეთი ინფორმაციის აღდგენაში გვეხმარება დამატებითი ელექტრონული ფოსტის მისამართების ან მობილური ნომრების მითითება.

ელექტრონული ფოსტის ანგარიშის ან ნებისმიერი სხვა ტიპის ანგარიშის გახსნისას, ორგანიზაციები გვთავაზობენ დამატებითი „საიდუმლო კითხვების“ გამოყენებას, რისი მიზანიც ანგარიშის უსაფრთხოების მაღალი დაცულობის გარანტირებაა. კითხვები შეიძლება იყოს მაგალითად, დაბადების თარიღი, შინაური ცხოველის სახელი და ასე შემდეგ. ვინაიდან ინტერნე სივრცეში ყველანაირი პერსონალური ინფორმაცია ხელმისაწვდომია, სასურველია ამ კითხვებზე გასაცემი პასუხებიც ისე აღვიქვათ, როგორც კიდევ ერთი პაროლი.

უსაფრთხოების დამატებითი ზომების გამოყენება საფრთხეებს ამცირებს, თუმცა გარკვეული საფრთხეები მაინც არსებობს. უსაფრთხოების დამატებითი ზომების მიღება

უბრალოდ საქმეს ურთულებს კიბერკრიმინალებს. ორგანიზაციებსა და ბანკებთან თანამშრომლობის დაწყებამდე გაარკვიეთ, რა უსაფრთხოების მექანიზმებს გამოიყენებენ ისინი, მომხმარებელთა პერსონალური ინფორმაციის დასაცავად და რაც მთავარია, გამოიყენეთ ორმაგი ავთენთიფიკაცია მეტი დაცულობისთვის.

დანართი 3

რჩევები სახლში უსაფრთხო კიბერგარემოს შესაქმნელად

რჩევები სახლში უსაფრთხო კიბერგარემოს შესაქმნელად

1. საკუთარი თავის თავდაცვა

თუ თქვენს მიერ მიღებული შეტყობინება/ტელეფონში შემოსული ზარი საეჭვოა ან ზედმეტად კარგი ჩანს იმისთვის, რომ რეალობა იყოს შესაძლებელია თქვენ შეტევის მსხვერპლი ხართ. მაგალითები:

- ფიშინგის შემცველი ელ. წერილები ინტერნეტ თაღლითობის ფორმაა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პერსონალური მონაცემები. მსგავსი მეილის ადრესატად შეიძლება მოგვევლინოთ მეგობარი, ოჯახის წევრი ან თქვენთვის კარგად ნაცნობი ორგანიზაცია. კიბერკრიმინალს შეუძლია თქვენი სოციალური ქსელების საშუალებითაც კი მიიღოს მისთვის საჭირო ინფორმაცია.
- შესაძლებელია დაგირეკოთ უცნობმა პიროვნებამ, გაგეცნოთ როგორც კომპანია Microsoft-ის ტექნიკური მხარდამჭერის ჯგუფის წევრი და გაგანობოთ, რომ თქვენი კომპიუტერი დაინფიცირებულია. აღნიშნული პიროვნება შეიძლება კიბერკრიმინალი აღმოჩნდეს, რომლის მიზანია თქვენს კომპიუტერზე წვდომის მოპოვება ან ყალბი ანტივირუსული პროგრამული უზრუნველყოფის გაყიდვა.

2. სახლის უკაბელო ინტერნეტის უსაფრთხოება

WI-FI -ის როუტერი არის ფიზიკური მოწყობილობა, რომლის მეშვეობითაც ხდება WI-FI -ს ქსელთან დაკავშირება.

ხშირად უკაბელო ინტერნეტს ქარხნულად აქვს დაყენებული პაროლი, რომლის გამოცნობა მარტივია ჰაკერებისთვის, მითუმეტეს თუ მათ როუტერის სახელი იციან. სწორედ ამიტომ საჭიროა მისი შეცვლა ძლიერი პაროლით, რომელიც მხოლოდ თქვენ გეცოდინებათ.

WI-FI -ს ქსელი დააყენეთ ისე, რომ მას ქონდეს საიმედო პაროლი, გამოიყენეთ უკაბელო ქსელის ყველაზე ძლიერი შიფრაციის მეთოდი, WPA2.

აუცილებელია გქონდეთ ინფორმაცია ყველა მოწყობილობის შესახებ, რომელიც თქვენ ინტერნეტ ქსელთან არის დაკავშირებული (მაგ. ტელევიზორი, სათამაშო კონსოლები და მანქანაც კი).

3. თქვენი კომპიუტერების/მოწყობილობების უსაფრთხოება

რამდენიმე ნაბიჯი თქვენი სახლის ინტერნეტ ქსელთან დაკავშირებული მოწყობილობების დასაცავად.

დარწმუნდით რომ აღნიშნული მოწყობილობები დაცულია ძლიერი პაროლის მეშვეობით და მუდმივად განაახლეთ პროგრამული უზრუნველყოფის უკანასკნელი ვერსიით, თუ შესაძლებელია დააყენეთ მისი ავტომატური განახლება.

კომპიუტერებს უნდა ჰქონდეთ დაყენებული ანტივირუსის და Firewall-ის უახლესი ვერსიები.

კომპიუტერის თუ მობილური მოწყობილობის უტილიზაციამდე დარწმუნდით, რომ წაშლილი გაქვთ ყველანაირი პერსონალური ინფორმაცია, მობილური ტელეფონის შემთხვევაში აირჩიეთ მოწყობილობის უსაფრთხო გადატვირთვის ოფცია.

4. თქვენი ანგარიშების / პაროლების უსაფრთხოება

რამდენიმე რჩევა თქვენი სხვადასხვა ანგარიშის (ონლაინ ანგარიში, კომპიუტერის და მოწყობილობის ანგარიში) დასაცავად.

ყოველთვის გამოიყენეთ გამოსაცნობად რთული, გრძელი პაროლები, ასევე სადაც შესაძლებლობა გექნებათ საიდუმლო ფრაზები (passphrases). მსგავსი პაროლები სხვადასხვა სიტყვებისგან არის შემდგარი, როგორიც არის „საღ არის ჩემი ყავა?".

თითოეულ თქვენს ანგარიშზე და მოწყობილობაზე გამოიყენეთ სხვადასხვა პაროლები. თუ სიმრავლის და სირთულის გამო მათი დამახსოვრება რთულია გირჩევთ გამოიყენოთ პაროლის მენეჯმენტის აპლიკაცია. ეს უკანასკნელი არის კომპიუტერული პროგრამა, რომელიც დაშიფრულ საცავში (encrypted vault) უსაფრთხოდ ინახავს ყველა პაროლს.

სადაც შესაძლებლობა გექნებათ ყველგან გამოიყენეთ ორმაგი ავთენტიფიკაციის მეთოდი რომელიც გულისხმობს, რომ ანგარიშზე შესასვლელად პაროლთან ერთად დაგჭირდებათ დამატებითი კოდი (როგორიც არის კოდი, რომელიც გამოგზავნილი იქნება სმარტფონზე).

სოციალურ ქსელში გამოაქვეყნეთ მხოლოდ ის ინფორმაცია რაც გსურთ, რომ იყოს საჯარო.

5. ნაბიჯები, რომლებიც უნდა გადადგათ თუ კიბერშეტევის მსხვერპლი გახდით

დაცულობის დონის მიუხედავად ადრე თუ გვიან შესაძლებელია, რომ გახდეთ კიბერშეტევის მსხვერპლი.

რეგულარულად შექმენით თქვენი პერსონალური მონაცემების სარეზერვო ასლები (backups). თუ თქვენი კომპიუტერი/მობილური მონაცემები გახდა კიბერშეტევის მსხვერპლი ერთადერთი გზა თქვენი პერსონალური ინფორმაციის აღსადგენად შეიძლება სარეზერვო ასლები იყოს.

თუ თქვენი ონლაინ ანგარიშებიდან ერთ-ერთი გახდა კიბერშეტევის მსხვერპლი აუცილებლად უნდა შეხვიდეთ და პაროლი შეცვალოთ უფრო ძლიერით და უნიკალურით. თუ თქვენ წვდომის საშუალება არ გაგაჩნიათ მაშინ დაუკავშირდით თავად კომპანიას.

აკონტროლეთ თქვენი საკრედიტო ბარათები, თუ თქვენ ნახავთ საეჭვო ხარჯებს, სასწრაფოდ დაუკავშირდით საკრედიტო ბარათის კომპანიას.

დანართი 4

ბავშვების დაცვა ინტერნეტ სივრცეში

ინტერნეტი და კომპიუტერი ჩვენი ყოველდღიურობის განუყოფელ ნაწილად იქცა და რაც არ უნდა დატვირთულები ვიყოთ, მაინც ვიტოვებთ დროს ეკრანის წინ გასატარებლად. იმ ფაქტორების გათვალისწინებით, როგორიცაა ბავშვური ცნობისმოყვარეობა და მიამიტობა, არ არის მიზანშეწონილი უსაფრთხოების იდენტური პრაქტიკის გამოყენება ზრდასრული მომხმარებლისა და მოზარდის შემთხვევაში.

ონლაინ დამნაშავეები განსაკუთრებულ საფრთხეს წარმოადგენენ ბავშვებისთვის. ინტერნეტი ანონიმური სივრცეა, რომელიც შესაძლებლობას იძლევა თავი გაასაღო სხვა პიროვნებად, ან უბრალოდ შენიღბო შენი იდენტობა. ზრდასრული ადამიანები ხშირად ხდებიან მსგავსი ბოროტმოქმედების მსხვერპლნი, თუმცა ბავშვების წამოგება მაქინაციებზე ბევრად ადვილია.

რა შეგვიძლია გავაკეთოთ მსგავსი ინციდენტების ასაცილებლად

- თვალი ადევნეთ თქვენი შვილის აქტივობას ინტერნეტ სივრცეში და დაეხმარეთ მას კომპიუტერის მოხმარების უნარჩვევების გამომუშავებაში.
- განათავსეთ კომპიუტერი თქვენთვის ხილულ სივრცეში, რათა მუდმივად შეძლოთ მისი მონიტორინგი. ასე ბავშვი მოერიდება ისეთი ვებ გვერდების სტუმრობას ან ისეთი აქტივობის განხორციელებას რომელსაც ვუკრძალავთ.
- გააფრთხილეთ ბავშვი მოსალოდნელი საფრთხეების თაობაზე, დარწმუნდით რომ თქვენმა შვილმა იცის ინტერნეტში დასაშვები აქტივობის ზღვარი და ის მას არ გადალახავს. აუცილებელია შეიზღუდოს კომპიუტერთან ურთიერთობის დრო.
- მნიშვნელოვანია ბავშვებს ვესაუბროთ ინტერნეტ საფრთხეებზე, რათა მათ შეძლონ საეჭვო ქცევის ან აქტივობის აღმოჩენა. დარწმუნდით რომ ბავშვთან საუბრისას შეეხეთ ისეთ თემებსაც როგორიცაა სოციალური ქსელები და კიბერბულინგი. ეცადეთ არ დააშინოთ მოზარდი, უბრალოდ დაანახეთ მხოლოდ ნაცნობ ადამიანებთან კომუნიკაციის დადებითი თვისებები.
- მუდმივად ამოწმეთ მისი აქტივობა. საძიებო ისტორიის შემოწმებით თქვენ მოიპოვებთ ინფორმაციას იმის თაობაზე თუ ვისთან აქვს თქვენ შვილს კონტაქტი და რა ინფორმაციის მოპოვებას ცდილობს ინტერნეტის მეშვეობით.
- იყავით მაქსიმალურად ღია შვილებთან ურთიერთობაში, რათა ინტერნეტის მოხმარებასთან დაკავშირებული კითხვების შემთხვევაში, მათთვის არ იქმნებოდეს ბარიერი თქვენთან კომუნიკაციის დროს.
- გამოიყენეთ სხვადასხვა ანგარიშები კომპიუტერის მოხმარებისას. აღნიშნული დაგიცავთ გარკვეული ფაილების წაშლისგან და განადგურებისგან, ხოლო მოზარდის შექმნილ ანგარიშზე შეძლებთ პრივილეგიის შეზღუდვას თუ თვლით რომ ეს მისთვის საზიანოა.

- დანერგეთ მშობლის კონტროლის მექანიზმები: მაგალითად ინტერნეტ ბრაუზერები საშუალებას გაძლევთ დაბლოკოთ თქვენთვის არასასურველი შინაარსის მქონე ვებ გვერდები. ხოლო პარამეტრებს შეგიძლიათ დაადოთ პაროლი და თქვენი ნებართვის გარეშე ეს შეზღუდვები არ მოიხსნება.

დანართი 5

თავდაცვა რეალური კიბერსაფრთხეებისგან

რატომაა სიფრთხილე აუცილებელი

ჩვენი ყოველდღიურობა ინტერნეტის გარეშე წარმოუდგენელია. ინტერნეტი არის ინფორმაციის მიღების, გაცემისა და კომუნიკაციის ყველაზე მნიშვნელოვანი არხი. ინტერნეტს უამრავი დანიშნულებით ვიყენებთ, დაწყებული ახალი ამბების მიღებით, დამთავრებული - საქმიანი და მეგობრული მიმოწერით. ინტერნეტის გამოყენებისას ისეთივე სიფრთხილე უნდა გამოვიჩინოთ, როგორსაც რეალურ ცხოვრებაში ვიჩენთ. აუცილებელია იმ პირთა ცნობიერების ამაღლება, რომელთათვისაც ინტერნეტის გამოყენება გარკვეულ სირთულეებთანაა დაკავშირებული და ახალ გამოწვევად ითვლება.

რა უნდა გვახსოვდეს

გახსოვდეთ, ინტერნეტი თავისუფალი სივრცეა, სადაც ყველა პიროვნებას სურვილისამებრ შეუძლია ამა თუ იმ ინფორმაციის გამოქვეყნება. სანამ ინფორმაციას დაიჯერებთ ან გაიზიარებდეთ, დარწმუნდით წყაროს სანდოობაში. გახსოვდეთ რომ, კიბერკრიმინალებს შეუძლიათ სხვა პირის განსახიერება ელექტრონული ფოსტის ან სხვა საკომუნიკაციო ქსელის საშუალებით. იმისთვის, რომ შესაძლო პრობლემები თავიდან ავიცილოთ, აუცილებელია დავაზუსტოთ ჩვენს ფოსტაზე შემოსული წერილის ადრესატის ვინაობა და არ გავცეთ პერსონალური ინფორმაცია დაუფიქრებლად.

არ დაუჯეროთ ელექტრონულ ფოსტაზე შემოსულ წერილებს, სადაც რაიმე არარეალურ დაპირებას გასცემენ. მაგალითად მომხმარებლებს ხშირად მისდით წერილები ლატარეაში გამარჯვების ან რაიმე დიდი მემკვიდრეობის მიღების თაობაზე. ესეთი წერილები დიდი ალბათობით სპამი ან ფიშინგია. უფრთხილდით ასევე სარეკლამო Pop-Up ფანჯრებს, რომლებიც უფასოდ გთავაზობენ პროგრამული უზრუნველყოფის გადმოწერას, რადგან ამ გზით შესაძლოა გაუცნობიერებლად ჯაშუშური პროგრამა დააინსტალიროთ.

ზოგიერთ საფოსტო სერვისს გააჩნია ავტომატური ფუნქცია, რომელიც შემოსულ წერილზე პასუხად იტყობინება, რომ ადრესატი რომელსაც წერილს უგზავნიდით „გასულია“ ~(იგულისხმება იმყოფება საზღვარგარეთ და ა.შ.) არ არის სასურველი თქვენი გამგზავრების და მითუმეტეს თქვენი ადგილმდებარეობის შესახებ ინფორმაცია საჯარო იყოს.

შექმენით სარეზერვო ასლი, რათა კომპიუტერის დაზიანების, დაინფიცირების ან დაკარგვის შემთხვევაში თქვენი ინფორმაცია შეგენახოთ.

დაადეთ საიმედო პაროლი თქვენს პერსონალურ კომპიუტერს, მუდმივად განაახლეთ ანტივირუსი, დააყენეთ ე.წ. ეკრანის დამცავი იგივე „Screensaver”.

დანართი 6

უსაფრთხოების ზომები, რომელიც კომპიუტერის ინტერნეტთან დაკავშირებამდე უნდა გავითვალისწინოთ

რატომაა კომპიუტერის უსაფრთხოება ასეთი მნიშვნელოვანი?

კომპიუტერში ვანთავსებთ პერსონალურ და ფინანსურ ინფორმაციას. შესაბამისად კომპიუტერის უსაფრთხო ფუნქციონირებაზე ზრუნვა ჩვენთვის უმნიშვნელოვანესი უნდა იყოს.

რა გავაკეთოთ კომპიუტერის უსაფრთხო ფუნქციონირებისთვის?

აუცილებელია უსაფრთხოების გარკვეული ზომების მიღება, თუმცა უსაფრთხოების არცერთი ზომა არ არის ჩვენი დაცულობის ასპროცენტიანი გარანტი.

გააქტიურეთ და დააკონფიგურირეთ თქვენი ბრანდმაუერი (Firewall) - ბრანდმაუერი (firewall) აპარატულ–პროგრამული ტიპის ქსელური კონფიგურაციაა, რომელიც, პროქსი–სერვერთან ერთად, უსაფრთხოების ბარიერს ჰქმნის ბრანდმაუერით დაცულ ლოკალურ ქსელსა და ინტერნეტს შორის და ამცირებს არასანქცირებული შემოჭრის საფრთხეს. ბრანდმაუერში არასასურველი ცვლილებების განხორციელების თავიდან აცილების მიზნით, დააყენეთ რთულად გამოსაცნობი პაროლი.

დააინსტალირეთ ანტივირუსი - პროგრამა, რომელიც გამოიყენება მავნე პროგრამებისგან თავის დასაცავად. დღეისთვის ინფორმაციული უსაფრთხოების სფეროს მრავალი კომპანია ინტერნეტ-მომხმარებელს სთავაზობს ანტივიერუსულ პროგრამულ უზრუნველყოფას, მათ შორის უფასო პროდუქტს. სასურველია ანტივირუსებს ავტომატური განახლების ფუნქცია ჩავურთოთ.

წაშალეთ პროგრამები რომელთაც არ იყენებთ - კიბერკრიმინალები ეძებენ მოწყვლადობებს პროგრამულ უზრუნველყოფებში. თვალი გადაავლეთ თქვენს მიერ დაინტალირებულ პროგრამებს და წაშალეთ ისინი, რომლებიც აღარ გესაჭიროებათ.

იმოქმედეთ უკანასკნელი პრივილეგიის პრინციპით - მავნე პროგრამული უზრუნველყოფა მოქმედებს მომხმარებლის პრივილეგიის ფარგლებში, რაც უფრო შეზღუდულ წვდომას დავუშვებთ ჩვენს ელექტრონულ მოწყობილობაზე, მით ნაკლები საფრთხის წინაშე დავდგებით.

მოახდინეთ პარამეტრების მოდიფიკაცია - პარამეტრების გარკვეული მოდიფიცირება ამცირებს ბოროტმოქმედების შესაძლებლობას განახორციელონ კიბერშეტევა.

დამატებითი უსაფრთხოების ზომები

- გამოიჩინეთ სიფრთხილე ელექტრონულ ფოსტაზე მიმაგრებულ ფაილებთან
- გამოიყენეთ ძლიერი პაროლები
- გამოიჩინეთ სიფრთხილე ინფორმაციის გაცემისას

დანართი 7

რა არის ელექტრონული მედია მატარებელი და რა რისკებთანაა დაკავშირებული მისი გამოყენება?

ელექტრონული მედია მატარებელი (USB ფლეშკა) არის ელექტრონული ინფორმაციის პორტატული დამგროვებელი, რომელიც გამოირჩევა მცირე ზომითა და ღირებულებით. ის დღეისთვის კომპიუტერის მომხმარებელთათვის ყველაზე მოსახერხებელი საშუალებაა. USB საკმაოდ პატარა, პორტატული და იაფი საშუალებაა, ინფორმაციის შენახვისა და გადატანისთვის, თუმცა მოწყობილობის ეს მახასიათებლები, მას კიბერდამნაშავეებისთვისაც მიმზიდველს ხდის.

კიბერკრიმინალებს შეუძლიათ ელექტრონული მედია მატარებელი მავნე პროგრამული უზრუნველყოფით დააინფიცირონ და მისი კომპიუტერზე შეერთებისას კომპიუტერიც დაინფიცირდება.

კიბერკრიმინალს ფიზიკური წვდომა თუ აქვს თქვენს კომპიუტერთან, ელექტრონული მედია მატარებელით ინფორმაციის მოპარვა გაუადვილდება. ელექტრონულ მოწყობილობასთან მედია მატარებლის მიერთებით, ის სწრაფად გადმოწერს მისთვის სასარგებლო ინფორმაციას. ასეთ დროს გამორთული კომპიუტერიც კი მოწყვლადია, რადგან კომპიუტერის მეხსიერება ძაბვის გათიშვის შემდეგაც ფუნქციონირებს რამდენიმე წუთი. თუ ბოროტმოქმედს აქვს ფიზიკური წვდომა თქვენს კომპიუტერზე და შეუძლია მედია მატარებელი შეაეთოს იმ მომენტში, როცა კომპიუტერი ახალი გამორთულია, ის შეძლებს მოკლე დროში გადმოაკოპიროს თქვენი კომპიუტერის მეხსიერება. მსხვერპლი შეიძლება ვერც კი მიხვდეს რომ მისი კომპიუტერი დაჰაკეს.

ელექტრონულ მედია მატარებელთან დაკავშირებული ერთ-ერთი ყველაზე დიდი საფრთხე მაინც ის არის, რომ იგი ადვილი დასაკარგი და მოსაპარია. თუ ე.წ. ფლეშკაზე არსებული მონაცემები არ არის დაშიფრული, მის გამოყენებას შეძლებს ნებისმიერი, ვის ხელშიც ჩავარდება მოწყობილობა.

როგორ დავიცვათ მონაცემები?

- არ შეაერთოთ გაურკვეველი წარმომავლობის ელექტრონული მედია მატარებელი თქვენს კომპიუტერს;
- გამოიყენეთ დაშიფვრა და პაროლები თქვენს მედია მატარებელზე, რათა მისი დაკარგვის შემთხვევაში თქვენი მონაცემები დაცული იყოს;
- სამსახურეობრივი და პირადი მიზნებისთვის სხვადასხვა მედია მატარებელი გამოიყენეთ და მეტი სიფრთხილით მოეკიდეთ იმ მოწყობილობას, რომელზეც კორპორაციულ ინფორმაციას ინახავთ, რადგან მისი გამჟღავნებით შეაძლოა საფრთხე შეუქმნათ თქვენს დამქირავებელ ორგანიზაციას;
- მოახდინეთ ავტომატური გახსნის ფუნქციის დეაქტივაცია, რადგან როცა ფუნქცია არ არის დეაქტივირებული, USB-ის, CD-ის ან DVD დისკის შეერთებისას ავტომატურად იხსნება ყველა ის ფაილი რაც მასზეა მოთავსებული, შესაბამისად იზრდება კომპიუტერის დაინფიცირების რისკებიც;

- მუდმივად განაახლეთ პროგრამული უზრუნველყოფა (ანტივირუსი, ანტიჯაშუშური პროგრამა, ბრანდმაუერი და ა.შ.)

დანართი 8

ვებ-ბრაუზერის კონფიგურაციის გამართვა

კომპიუტერებზე დაყენებულია ვებ-ბრაუზერები (Internet Explorer, Opera, Chrome, Mozilla Firefox, Apple Safari). ვინაიდან ისინი განსაკუთრებით ხშირად გამოიყენება, საჭიროა მათი კონფიგურირება უსაფრთხოების მოთხოვნების შესაბამისად. ხშირად ახლად დაყენებულ ვებ-ბრაუზერებში არ არის გააქტიურებული უსაფრთხოების საშუალებები და ფუნქციები. დაუცველი ბრაუზერის მეშვეობით შესაძლებელია, პერსონალური მონაცემების დაკარგვა, კომპიუტერის დაინფიცირება, დაზიანება და ა.შ. აუცილებელია ასევე იმის შემოწმება თუ რამდენად გამართულია კონფიგურაცია უსაფრთხოების თავალსაზრისით. ვინაიდან ვებ-ბრაუზერები კიბერ-შეტევების ერთ-ერთი უმთავრესი და ყველაზე გავრცელებული ვექტორია, საჭიროა მათი ფუნქციონირების მუდმივი მონიტორინგი.
ყველა ბრაუზერს განსხვავებული პარამეტრები აქვს. მაგალითად Microsoft Internet Explorer -ში პარამეტრების შესაცვლელად საჭიროა შემდეგი მოქმედებების შესრულება: Tools -> Internet Options, ხოლო მაგალითად Firefox-ში :Tools-Options და ამგვარად შევძლებთ არასასურველი ფაილების ავტომატურად შენახვის ფუნქციის გათიშვას, არასასურველი დამატებების დაყენების პრევენციას და ა.შ. ყველა ბრაუზერის პარამეტრები განსხვავდება და მათში ცვლილებების შეტანა სხვადასხვანაირად ხდება.

რა პრინციპით უნდა ვიმოქმედოთ პარამეტრების დაყენებისას?

საუკეთესო გამოსავალია გაამკაცროთ უსაფრთხოების ნორმები. თუმცა ზოგჯერ გარკვეული მახასიათებლების შეზღუდვამ შეიძლება ზოგიერთი ვებ – გვერდის გამართული ფუნქციონირება შეაფერხოს.

განსხვავებულ ბრაუზერებში განსხვავებული ტერმინები გამოიყენება, ჩვენ წარმოგიდგენთ ზოგიერთ მათგანს:

სივრცე - თქვენი ბრაუზერი გაძლევთ შესაძლებლობას ვებ გვერდები დაყოთ სხვადასხვა სეგმენტებად და თითოეული სეგმენტისთვის შეგიძლიათ განსხვავებული შეზღუდვები გამოიყენოთ. მაგალითად Internet explorer-ი განსაზღვრავს შემდეგ სეგმენტებს.

ინტერნეტი - ინტერნეტი აღნიშნავს გლობალურ კომპიუტერულ ქსელს, რომელიც ეფუძნება IP პროტოკოლს და პაკეტთა მარშრუტიზაციას. ინტერნეტი ქმნის გლობალურ საინფორმაციო სივრცეს და წარმოადგენს მსოფლიო ქსელის საფუძველს. მისი გამოყენებისას უსაფრთხოების მკაცრი ზომები უნდა იქნეს მიღებული.

ლოკალური ქსელი - კომპიუტერული ქსელი, შემდგარი ფიზიკურად ერთმანეთთან ახლოს მდგომი კომპიუტერებისაგან, რომლებიც ერთობლივად იყენებენ, აპარატურულ, პროგრამულ რესურსებსა და მონაცემებს. როგორც წესი ლოკალური ქსელის ერთი ან რამდენიმე კომპიუტერი ასრულებს ფაილების სერვერის ფუნქციას. მისი გამოყენებისას ნაკლებ სიფრთხილეს იჩენენ, თუმცა გასათვალისწინებელია, რომ ვირუსებმა მსგავსი ტიპის ქსელშიც შეიძლება შეაღწიოს და პრივილეგიების გაცემამდე დაფიქრება გვმართებს.

მაღალი სანდოობს მქონე ვებ გვერდები - ასეთი ტიპის ვებ გვერდებად უნდა მოვიაზროთ ისინი რომელთაც დანერგილი აქვთ SSL (Secure sockets layer) სერთიფიკატი, რადგან

აღნიშნული გვაძლევს საფუძველს ვიფიქროთ, რომ ვებ გვერდი ნამდვილად წარმოადგენს იმას რადაც თავს ასაღებს.

ვებ გვერდები, რომლებზეც გარკვეული შეზღუდვებია დაწესებული - ასეთ ვებ გვერდთა სიაში ძირითადად ისეთი ვებ გვერდები ხვდებიან, რომელთა სანდოობაშიც არ ვართ დარწმუნებული. სასურველია ასეთი ვებ გვერდები საერთოდ არ მოვინახულოთ.

ჯავასკრიპტი - პროგრამირების ერთ-ერთი ფართოდ გავრცელებული ენაა, იგი შეიძლება კომპიუტერული შეტევისთვისაც იქნეს გამოყენებული.

ქუქები - თუ არ გსურთ ქუქი-ფაილების მიღება, შეგიძლიათ ბრაუზერის პარამეტრებში აირჩიოთ, რომ მიიღოთ შეტყობინება, როდესაც გეგზავნებათ ქუქი-ფაილები, ან შეგიძლიათ საერთოდ უარი თქვათ ქუქი-ფაილების მიღებაზე. აგრეთვე, შეგიძლიათ წაშალოთ უკვე ჩაწერილი ქუქი-ფაილები.

Pop-up ფანჯრების დაბლოკვა - თქვენ შეგიძლიათ შეამციროთ იმ Pop up რეკლამების რაოდენობა, რომელთაც ყოველდღიურად იღებთ. გაითვალისწინეთ, რომ ზოგიერთი მათგანი შეიძლება მავნე კოდის შემცველიც იყოს.

დანართი 9

სმარტფონის უსაფრთხოება

თანამედროვე მობილურ ტელეფონებს დარეკვისა და სმს-ის მიღების ფუნქციის გარდა, აქვთ ინტერნეტთან დაკავშირების საშუალებაც. დამატებითი ფუნქციები მათ უფრო მიმზიდველს ხდის, თუმცა მსგავსი ტიპის ტელეფონებზე კიბერდამნაშავეების მიერ, შეტევების განხორციელების ალბათობაც მეტია.

ზოგიერთ ელექტრონულ მოწყობილობას აქვს ტექსტური შეტყობინებების მიღებისა და გაგზავნის ლიმიტი, შესაბამისად დიდი რაოდენობით სპამის მიღების შემთხვევაში ტელეფონის მფლობელს დამატებითი ხარჯების გაღება მოუწევს.

კიდევ ერთი საფრთხე რის წინაშეც შეიძლება მობილური ტელეფონის მფლობელი დადგეს, ფიშინგ შეტევაა, ახლა უკვე ელექტრონული ფოსტის გარდა ფიშერები სმს-ის სახითაც გზავნიან მავნე კონტენტის შემცველ წერილებს. წერილი, თითქოს გამოგზავნილია ბანკის, სერვისის პროვაიდერის ან სხვა ცნობილი ბრენდ ორგანიზაციის მიერ, რომელთანაც მომხმარებელს აქვს შეხება. წერილში რაიმე მიზეზით თხოვენ ადრესატს გაანახლოს თავისი პირადი მონაცემები მითითებული ბმულის საშუალებით. დასახელებული მიზეზი შეიძლება იყოს სხვადასხვაგვარი, მაგალითად ასეთი ყალბი წერილი შეიძლება იტყობინებოდეს, რომ მომხმარებლის ანგარიში იქნება შეჩერებული თუ არ მოხდა მისი პაროლის ან საკრედიტო ბარათის ინფორმაციის განახლება მოცემულ ვებ გვერდზე. ფიშერების კიდევ ერთი ხრიკი არის ბმულის URL მისამართები, რომელიც ძალიან ჰგავს ნამდვილი ვებ გვერდის სახელს და დაკვირვების გარეშე მომხმარებელმა შეიძლება ვერ შეამჩნიოს ასოების ცდომილება. ასევე ყალბი ვებ გვერდი შეიძლება იწყებოდეს IP მისამართით და გრძელდებოდეს ორგანიზაციის სახელით, ან მითითებული იყოს რაიმე სხვა ვებ გვერდი, რომელზეც მიბმულია სხვა ვებ გვერდის მისამართი.

კიბერდამნაშავეებს თქვენი მობილური ტელეფონის მეშვეობით შეუძლიათ სხვა მობილურ ტელეფონებზე განახორციელონ შეტევა. ამით ისინი წარმატებულად ფარავენ თავიანთ ვინაობას და პოტენციურ მსხვერპლთა რიცხვიც იზრდება.

მობილური ტელეფონებით ჩვენ ყოველდღიურად ვახორციელებთ სხვადასხვა სახის ფინანსურ ტრანზაქციებს. კიბერდამნაშავე, რომელიც მოიპოვებს ჩვენს მობილურ ტელეფონზე წვდომას ასევე მოიპოვებს წვდომას ჩვენს ინტენეტ ბანკსა და პაროლებზე. იგი ამ ინფორმაციას თავის პირადი სარგებლისთვის გამოიყენებს.

როგორ დავიცვათ თავი

სასურველია ჩვენი მობილური ტელეფონი იმავე მეთოდებით დავიცვათ, რა მეთოდებითაც ჩვენი კომპიუტერის უსაფრთხოებას ვიცავთ.

არ გაასაჯაროვოთ თქვენი მობილური ტელეფონის და ელექტრონული ფოსტის მისამართები, რაც მეტმა ადამიანმა იცის თქვენი მონაცემები მით მეტია შანსი რომ მსგავსი შეტევების სამიზნე გახდეთ.

არ გადახვიდეთ ტექსტურ შეტყობინებაში და ელ ფოსტაზე მიღებულ საეჭვო ლინქებზე.

მუდმივად აკონტროლეთ თქვენი პარამეტრები, თქვენს მობილურზე გააქტიურებული ბლუთუს ფუნქცია შეიძლება საფრთხის შემცველი იყოს თქვენთვის, ამიტომ გამორთეთ ის როცა არ იყენებთ.

სიფრთხილე გამოიჩინეთ პროგრამული უზრუნველყოფის ჩამოტვირთვისას. არ ენდოთ გაურკვეველი წარმომავლობის ვებ გვერდებს. არ დაიზაროთ ვებ გვერდის სერტიფიკატის შემოწმება. პროგრამის გახსნამდე გადმოწერეთ ის კომპიუტერში და შეამოწმეთ ვირუსებზე.

დანართი 10

სოციალური ქსელის უსაფრთხოება

სოციალური ქსელი ეს არის საკომუნიკაციო სერვისი, რომელთან წვდომაც ინტერნეტის გამოყენებითაა შესაძლებელი.

სოციალური ქსელების საშუალებით ადვილია გავუზიაროთ ერთმანეთს ჩვენი ინტერესები, შეხედულებები, გავიჩინოთ მეგობრები, მოვძებნოთ ნაცნობები, ან დავამყაროთ ბიზნეს კომუნიკაციები.

ქსელში შექმნილია ჯგუფები რომლებიც საერთო ინტერესის გარშემო არიან გაერთიანებულნი.

სოციალური ქსელების ფუნქციონირება დამყარებულია კავშირებსა და კომუნიკაციაზე, აქედან გამომდინარე ჩვენ თამამად ვუდგებით ჩვენი პერსონალური ინფორმაციის საზოგადოდ გაზიარების საკითხს. როცა საქმე პირადი ინფორმაციის გასაჯაროებას ეხება ადამიანები რეალურ ცხოვრებასთან შედარებით ნაკლებ სიფრთხილეს იჩენენ ინტერნეტ სივრცეში, რიგი მიზეზების გამო:

- ინტერნეტ სივრცე ანონიმურობის განცდას აჩენს;
- ფიზიკური ინტერაქციის არარსებობა ცრუ დაცულობის შეგრძნებას გვიჩენს;
- ხდება ინფორმაციის გაზიარება რომელსაც უნდა გაეცნონ მათი მეგობრები, მაგრამ გვავიწყდება, რომ ეს ინფორმაცია ხელმისაწვდომი შეიძლება სრულიად უცხო ადამიანთა ჯგუფისთვისაც იყოს.

ზემოხსენებული ვებ გვერდების პოპულარობაა, იმის მიზეზი რომ თავდამსხმელები სწორედ სოციალური ქსელების მეშვეობით ავრცელებენ მავნე კოდებს. საეჭვოა ის ვებ გვერდები რომლებიც მესამე მხარის მიერ შექმნილ აპლიკაციებს გვთავაზობენ. თავდამსხმელებს შეუძლიათ შექმნან აპლიკაციები რომელიც სრულიად უსაფრთხოს და ლეგალურს გავს, მაგრამ რეალურად თქვენს ელექტრონულ მოწყობილობას აინფიცირებს და სარგებლობს თქვენი ინფორმაციით, ისე რომ თქვენ ამის შესახებ არაფერი იცით.

როგორ დავიცვათ თავი?

ლიმიტირებულად გავაზიაროთ ჩვენი პერსონალური ინფორმაცია-არ გავასაჯაროვოთ ისეთი ინფორმაცია, რომელიც მოწყვლადს გაგვხდის, მაგალითად ინფორმაცია ჩვენს განრიგზე რუტინაზე ან მისამართები და ა.შ. გაიხსენეთ სანამ დაპოსტავთ, რომ ამ ინფორმაციას უცხო ადამიანებიც ნახულობენ და დაფიქრდით იმაზე თუ რამდენად მისაღებია ეს თქვენთვის.

დაიმახსოვრეთ ინტერნეტი ღია წყაროა-ყველა თქვენი კომენტარი, მინაწერი და სურათი იმის მიუხედავად წაშლით თუ არა თქვენ მას, შეიძლება მაინც ინახებოდეს სხვა პირთა ელექტრონულ მოწყობილობებში. ამიტომ კარგად დაფიქრდით სანამ სოციალურ ქსელში რამეს მოიმოქმედებდეთ

ერიდეთ უცხოებს-ინტერნეტი საქმეს უადვილებს ადამიანებს დამალონ თავიანთი იდენტობა ან სულაც თავი სხვა ადამიანად გაასაღონ. ეს რა თქმა უნდა გარკვეული

მიზნების მიღწევას ემსახურება მათი მხრიდან. მოახდინეთ იმ ადამიანთა წრის შეზღუდვა ვისაც თქვენთან დაკონტაქტება შეუძლია. თუ მაინც ეკონტაქტებით ადამიანებს რომელთაც არ იცნობთ არ გაანდოთ მათ ზედმეტი ინფორმაცია და მოერიდეთ მათთან პირისპირ შეხვედრას.

განეწყვეთ სკეპტიკურად-არ დაიჯეროთ ყველაფერი რასაც ონლაინ კითხულობთ. ადამინებმა შეიძლება სიცრუე დაწერონ ამა თუ იმ თემაზე და ისეც შეიძლება მოხდეს რომ ამას სხვის სახელს ამოფარებული ჩადიოდნენ. არაა აუცილებელი ეს მავნე განზრახვით ხდებოდეს. შეიძლება ეს ყველაფერი უბრალო გაუგებრობა ან ხუმრობაა. სანამ რაიმეს მოიმოქმედებდეთ ინტერნეტში წაკითხული ინფორმაციის საფუძველზე, დარწმუნდით მის სისწორეში.

მეტი დაცულობისთვის შეცვალეთ გარკვეული ფუნქციები პარამეტრებში- ჩვენ შეგვიძლია დავხუროთ პროფაილი უცხო პირებისთვის რათა მათ ვერ შეძლონ მსგავს ვებ გვერდებზე ჩვენი მოძებნა, თუმცა ესეც არ გვაძლევს 100 პროცენტიან გარანტიას, რომ ჩვენს მიერ გაზიარებული ინფორმაცია არასასურველ პირებამდე არ მივა, თანაც ვებ გვერდები ხშირად ცვლიან თავიანთ პარამეტრებს ამიტომ რეგულარულად ადევნეთ თვალი უსაფრთხოებისა და პერსონალურ პარამეტრებს.

ერიდეთ მესამე მხარის შექმნილ აპლიკაციებს-მათ შეიძლება ჩვენი კომპიუტერი დააინფიცირონ, პარამეტრებიდან განსაზღვრეთ აპლიკაციების მიერ ჩვენს ინფორმაციებზე წვდომის ხარისხი.

გამოიყენეთ ძლიერი პაროლი- გამოიყენეთ პაროლები რომლებიც არ არის ადვილად გამოცნობადი. შეადგინეთ იგი განსხვავებული ციფრების, ასოებისა და სიმბოლოებისგან

განაახლეთ პროგრამული უზრუნველყოფა: დააინსტალირეთ პროგრამული უზრუნველყოფის პატჩები (ე.წ. Software patches) რომელიც თავდამსხმელებს არ მისცემს შესაძლებლობას არსებული მოწყვლადობები გამოიყენონ შეტევისთვის. სასურველია დააყენოთ ავტომატური განახლება.

დააინსტალირეთ ანტივირუსი: ანტივირუსი არის პროგრამა, რომელიც გამოიყენება კომპიუტერისათვის საზიანო პროგრამებისაგან თავის დასაცავად.

დანართი 11

ინფორმაციის ონლაინ განთავსების რეკომენდაციები

რატომაა მნიშვნელოვანი გვახსოვდეს რომ ინტერნეტი საჯარო სივრცეა?

გლობალური კომუნიკაცია ხელმისაწვდომი გახდა, მსოფლიო კომპიუტერული ქსელის დახმარებით, რომელსაც ინტერნეტს ვეძახით. იგი საშუალებას გვაძლევს მოვიპოვოთ სასურველი ინფორმაცია ადამიანზე ან მოვლენაზე. ინტერნეტი ანონიმურობის განცდას გვიტოვებს, რაც ინტერნეტით კომუნიკაციას უფრო ადვილს ხდის ვიდრე ფიზიკურ კომუნიკაციას. მნიშვნელოვანია გვახსოვდეს, რომ სინამდვილეში ინტერნეტში არ ვართ ბოლომდე ანონიმურები და ჩვენზეც ისევე ადვილია ინფორმაციის მოპოვება, როგორც სხვა ნებისმიერ ადამიანზე. ინტერნეტი ზოგიერთისთვის იმდენად კომფორტული გახდა, რომ მათ ჩამოუყალიბდათ ინტერნეტში ქცევის არც ისე უსაფრთხო ჩვევები. მაგალითად, თუ ადამიანები ერიდებიან პერსონალური ინფორმაციის გაცემას ქუჩაში შემხვედრ უცხო პირზე, ინტერნეტსივრცეში პირიქით, ისინი ძალიან მარტივად აკეთებენ ამას. როგორც კი თქვენი პერსონალური ინფორმაცია მოსაზრებების, თუ რაიმე სხვა ფორმით განთავსდება ინტერნეტსივრცეში, მასზე წვდომას მოიპოვებს მსოფლიოში მცხოვრები ნებისმიერი ადამიანი. ამიტომ მნიშვნელოვანია დავფიქრდეთ, გვინდა თუ არა ეს?

რა გაიდლაინებს უნდა მივსდიოთ ინტერნეტში ინფორმაციის განთავსების დროს?

დარწმუნდით, რომ არ შეეგექმნებათ პრობლემა, ნებისმიერმა პირმა ნახოს ის ინფორმაცია, რომელსაც ასაჯაროებთ. უნდა გვახსოვდეს, რომ ზოგადად ინტერნეტი არ არის დახურული ფორუმი, რომელშიც მხოლოდ თანამოაზრეები ურთიერთობენ. თუ გვსურს, რომ ჩვენს მიერ განთავსებული ინფორმაცია საზოგადოების მცირე წრემ ნახოს, აუცილებელია ინფორმაციასთან წვდომის წესები შევზღუდოთ. ინტერნეტსივრცეში არსებობს ვებ-გვერდები, რომლებიც ინფორმაციასთან წვდომის შესაზღუდად იყენებენ პაროლებს და უსაფრთხოების სხვა მექანიზმებს, მაგრამ ეს ყველა ვებ-გვერდს არ ეხება.

მოერიდეთ ზედმეტი ინფორმაციის გაცემას. ვირტუალურ სიცრცეში არ განათავსოთ ისეთი ინფორმაცია, როგორიცაა ჰობი, სამუშაო ადგილი, ინფორმაცია სამეგობროზე, ოჯახზე და წარსულზე. აღნიშნული ინფორმაცია შეიძლება კიბერკრიმინალებმა თქვენს წინააღმდეგ გამოიყენონ.

დაიმახსოვრეთ, თქვენს მიერ გამოქვეყნებული ინფორმაცია ინახება. რა თქმა უნდა, შეგიძლიათ მოახდინოთ პოსტის რედაქტირება ან სულაც აიღოთ ის ვებ-გვერდიდან, მაგრამ პოსტის ორიგინალი ვერსია ერთ ადამიანს მაინც ექნება შენახული. დაფიქრდით მოსალოდნელ შედეგებზე, სანამ რაიმე ნაბიჯს გადადგამდეთ.

დანართი 12

რამდენად ანონიმურები ვართ ინტერნეტ სივრცეში?

რა ტიპის ინფორმაციის შეგროვება ხდება?

ვებ-გვერდის მონახულებისას, ინტერნეტ მომხმარებლის ანონიმურობა დაცული არ არის. ინფორმაციას, რომელიც გვერდის ადმინისტრატორისთვის ღია ხდება, განეკუთვნება:

IP მისამართები. ყველა კომპიუტერს თავის ინდივიდუალური IP მისამართი აქვს. თქვენს ელექტრონულ მოწყობილობას შეიძლება ორნაირი IP მისამართი ჰქონდეს, დინამიური ან სტატიკური. თუ სტატიკური IP მისამართი გაქვთ, ის უცვლელად რჩება, ხოლო თუ IP მისამართი დინამიურია, ეს ნიშნავს, რომ ინტერნეტ სერვის პროვაიდერს IP მისამართების ბლოკი აქვს და თითოეულ ჯერზე, როცა თქვენ ვებ-გვერდს ეწვევით ის IP ახალი მისამართს მოგანიჭებთ. თუ თქვენს ელექტრონულ მოწყობილობას განსაზღვრული სტატიკური IP მისამართი აქვს და გაიგოთ ინფორმაცია მის შესახებ, ეწვიეთ ვე-გვერდს: www.showmyip.com

დომეინის სახელი. ინტერნეტი დაყოფილია დომეინებად, თითოეული მომხმარებლის ანგარიში ასოცირებულია ერთ-ერთ ასეთ დომეინთან. დომეინის განსაზღვრა შესაძლებელია URL-ის დაბოლოებაზე დაკვირვებით. მაგალიათად ვებ-გვერდები, რომელიც ბოლოვდება .edu-თი მიანიშნებს იმაზე, რომ საგანმანათლებლო დაწესებულების ვებ-გვერდზე იმყოფებით, ხოლო მაგალითად ვებ-გვერდები, რომლებიც ბოლოვდება .gov-ით მიანიშნებს რომ გვერდი ეკუთვნის სამთავრობო უწყებას. ქვეყნებსაც აქვთ საკუთარი დომეინები, რომელიც ავტომატურად გვახვედრებს თუ რომელი ქვეყნის ვე- გვერდზე ვიმყოფებით.

პროგრამული უზრუნველყოფის დეტალები. ორგანიზაციებს შეუძლიათ განსაზღვრონ, თუ რომელი ვებ-ბრაუზერის რომელი ვერსიიდან ეწვიეთ ვებ-გვერდს. მათ ისიც კი შეუძლიათ განსაზღვრონ რომელ ოპერაციულ სისტემას იყენებთ ელექტრონულ მოწყობილობაზე.

გვერდების ნახვები. ორგანიზაციებისთვის, რომლებიც ვებ-გვერდს მართავენ, ფლობენ ინფორმაციას იმის თაობაზე თუ რომელ ვებ-გვერდს ეწვიეთ და რამდენი ხანი დაჰყავით მასზე.

როგორაა ეს ინფორმაცია გამოყენებული?

ზოგადად ასეთი ტიპის ინფორმაცია, ლეგიტიმური მიზნებისთვის გამოიყენება. მაგალითად ორგანიზაციები, რომლებიც ვებ-გვერდებს მართავენ, გამოიყენებენ ამ ინფორმაციას სტატისტიკის გენერირებისთვის. ამით ისინი უკეთ შეაფასებენ ვებ-გვერდის პოპულარობას და იმას თუ რომელი შინაარსობრივი მხარე უფრო ნახვადია და ა.შ.; შემდგომ კი ამ ინფორმაციას მომხმარებელთა ინტერესების შესაბამისად ვებ-გვერდის მოდიფიკაციისთვის გამოიყენებენ.

ამ ტიპის ინფორმაცია ასევე გამოიყენება მარკეტინგისთვის. თუ ვებ-გვერდი იყენებს ქუქის. ქუქი-ფაილები არის მცირე ზომის ტექსტური ფაილები, რომლებიც ინახება თქვენს კომპიუტერში, პლანშეტსა თუ მობილურ ტელეფონში. ისინი არ არის ზიანის მომტანი

კომპიუტერისთვის და არც უსაფრთხოებისთვის. ისინი შეძლებენ განსაზღვრონ სხვა ვებ-გვერდებიც, რომელსაც თქვენ ეწვიეთ და შესაბამისად დაადგინონ თქვენი ინტერესები და ამ ინტერესების შესაბამისად რეკლამა გაუკეთონ ამა თუ იმ პროდუქციას.

თუმცა არსებობს იმის შესაძლებლობაც, რომ ზოგიერთი ვებ-გვერდი ამ ინფორმაციას ბოროტი მიზნებისთვის გამოიყენებს. ისინი მოიპოვებენ წვდომას ფაილებზე, პაროლებზე ან თქვენს პერსონალურ ინფორმაციაზე, ეცდებიან ფინანსური ან რაიმე სხვა ტიპის მოგების მიზნით ეს ინფორმაცია თავიანთ სასიკეთოდ გამოიყენონ.

როგორ შევამციროთ ჩვენზე არსებული ინფორმაციის გაცემა?

სიფრთხილე გამოიჩინეთ პერსონალური ინფორმაციის გაცემისას, არ მიუთითოთ თქვენი საკრედიტო ან სადებიტო ბარათის მონაცემები, პაროლები, მისამართი და ასე შემდეგ.

შეამცირეთ ქუქები, თუ კიბერკრიმინალები მოახდენენ თქვენი კომპიუტერის კომპრომეტირებას, ისინი მოიპოვებენ იმ ინფორმაციასაც, რომელიც თქვენს „ქუქებში“ ინახება. სამწუხაროდ გვიჭირს იმ ზარალის ოდენობის გაცნობიერება, სანამ ასეთი ზარალი რეალურად არ მოგვადგება.

დაფიქრდით სანამ რაიმე ვებ გვერდს ეწვევით. თუ ის საეჭვოდ გამოიყურება დატოვეთ ის.

დანართი 13

ელ-ფოსტაზე მიმაგრებული ფაილებისგან თავის დაცვის წესები

რატომ უნდა გამოვიჩინოთ სიფრთხილე ე.წ. „Attachment"-ის გახსნისას ელექტრონულ ფოსტაზე მიმაგრებულ ფაილებს ბევრი დადებითი მახასიათებელი აქვს, რაც მას პოპულარულს ხდის, თუმცა ისინი შეიძლება კომპიუტერის კომპრომეტირების მიზეზიც გახდნენ.

ინტერნეტ მომხმარებლები ელექტრონულ ფოსტას მასობრივად იყენებენ - წერილების გადაგზავნა მარტივი და სწრაფი პროცესია, შესაბამისად მისი მეშვეობით ვირუსების გავრცელებაც ადვილია. ზოგიერთ ვირუსს აქვს უნარი გავრცელდეს ჩვენი ნებართვის გარეშე და თავისით გადაიგზავნოს ჩვენი ფოსტიდან ყველა იმ მისამართზე, რომელსაც ფოსტაში გადააწყდება (ფოსტის მისამართებს მოიპოვებს გაგზავნილ და შემოსულ წერილებში ან საფოსტო ცნობარში). თავდამსხმელებმა იციან, რომ ფოსტის მომხმარებლები ნაცნობი ადრესატისგან მიღებულ წერილს ზედმეტი სიფრთხილის გარეშე თითქმის ავტომატურად ხსნიან.

თავდამსხმელები ცდილობენ მომხმარებლის ინტერესებთან დაკავშირებული თემატიკის ფაილები დაგზავნონ - ელექტრონულ ფოსტაზე ნებისმიერი ტიპის ფაილის მიმაგრებაა შესაძლებელი, შესაბამისად თავდამსხმელებს აქვთ სრული თავისუფლება კონტენტის არჩევაში.

ფოსტის პროგრამებს მრავალნაირი ფუნქცია აქვთ - მაგალითად, შესაძლოა წერილზე მიმაგრებული ფაილი ავტომატურად ჩამოიტვირთოს, თუ ფაილი დავირუსებულია ჩვენი კომპიუტერის კომპრომეტაცია მოხდება.

რა შეგვიძლია გავაკეთოთ ყოველივე ზემოთხსენებულისგან თავდასაცავად - უფრთხილდით წერილებს მიმაგრებული ფაილებით, თუნდაც ის ახლობელი ადამიანისგან მიიღოთ. ყოველთვის დაკვირვებით შეამოწმეთ წერილის ადრესატის მისამართი, შეიძლება გეგონოთ რომ მიღებული წერილი თქვენი მეგობრისგან ან უფროსისგან არის, მაგრამ ხანდახან ეს ასე არ არის. დარწმუნდით ადრესატის ვინაობაში და მხოლოდ ამის შემდეგ გახსენით ფაილი. ხშირად წერილები იგზავნება ვითომდა ჩვენი პროგრამული უზრუნველყოფის მომწოდებლისგან. დაიმახსოვრეთ, ვენდორები პატჩს და პროგრამულ უზრუნველყოფას ელექტრონულ ფოსტაზე არ აგზავნიან.

მიჰყევით თქვენს ინსტინქტებს: თუ თვლით, რომ წერილი საეჭვოდ გამოიყურება, არ გახსნათ. პირადად დაუკავშირდით გამომგზავნ პირს და მასთან გადაამოწმეთ, ისაა რეალური გამომგზავნი თუ მის სახელს ამოფარებული ბოროტმოქმედი. ხანდახან ანტივირუსები არ გვაძლევენ გაფრთხილებას ვირუსის არსებობის შესახებ, რადგან შეიძლება ვირუსი „ახალი თაობის" იყოს და ჩვენმა ანტივირუსმა მისი ხელწერა არ იცოდეს.

ნებისმიერი ფაილი გახსნამდე დაასკანერეთ - თუ არ გაქვთ საშუალება პირადად გადაამოწმოთ წერილის ადრესატთან ინფორმაცია ფაილის შესახებ, მაშინ საკუთარი უსაფრთხოების უზრუნველსაყოფად გაიარეთ შემდეგი საფეხურები:

1. განაახლეთ ანტივირუსი;

2. შეინახეთ ფაილი დისკზე;
3. შეამოწმეთ ფაილი განახლებული ანტივირუსით;
4. თუ დარწმუნდით რომ ფაილი სუფთაა, გახსენით იგი.

გამორთეთ ავტომატურად გადმოწერის ფუნქცია - მიღებული წერილების კითხვის პროცესის გასამარტივებლად პროგრამა გვთავაზობს წერილების ავტომატურად გადმოწერის და შენახვის ფუნქციას. თუ თქვენ ეს ფუნქცია გააქტიურებული გაქვთ, შედით პარამეტრებში და გამორთეთ.

შექმენით განცალკევებული ანგარიშები თქვენს კომპიუტერზე - ოპერაციული სისტემა გაძლევთ შესაძლებლობას შექმნათ რამდენიმე ანგარიში სხვადასხვა პრივილეგიით. თქვენს ფოსტაზე მოსულ წერილებს გაეცნობით იმ ანგარიშზე, სადაც შეზღუდული პრივილეგია გაქვთ, რადგან ზოგ ვირუსს ადმინისტრატორის პრივილეგია სჭირდება კომპიუტერის დასაინფიცირებლად, ასე კი უფრო მეტად დაცულები ვართ.

დანართი 14

სპამი

რა არის სპამი ?

სპამი არის ელექტრონული წერილის ტიპი, რომელიც იგზავნება პიროვნების ან კომპანიის მიერ, მიმღების დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა. პიროვნებას, რომელიც მსგავს წერილებს გზავნის ეწოდება სპამერი. მათი ძირითადი მიზანია თავიანთი პროდუქტის პოპულარიზაცია.

როგორ შევამციროთ ელექტრონულ ფოსტაზე მიღებული სპამების რაოდენობა?

არ გამოაქვეყნოთ თქვენი ელ-ფოსტის მისამართი ვებ-გვერდზე ან ფორუმზე, რადგან სპამ-ბოტები ათვალიერებენ ვებ-გვერდებს და ელ-ფოსტის მისამართის პოვნისას ავტომატურად შეაქვთ სპამ-სიაში;

შეამოწმეთ უსაფრთხოების პოლიტიკა - სანამ ელექტრონული ფოსტის მისამართს რომელიმე ვებ-გვერდზე მიუთითებდეთ, გაეცანით მათი უსაფრთხოების პოლიტიკას (Privacy Policy). ასეთ შემთხვევაში, წინასწარ გეცოდინებათ როგორ გამოიყენებს თქვენს პერსონალურ ინფორმაციას ვებ-გვერდი;

არ უპასუხოთ სპამ-წერილებს - პასუხის გაცემით თქვენ ადასტურებთ, რომ თქვენი ელ-ფოსტის მისამართი არის აქტიური და ამის შემდეგ უფრო მეტი არასასურველი წერილი მოგივათ;

არ გაუგზავნოთ სპამი სხვა მომხმარებლება - პასუხისმგებლობით მოეკიდეთ თქვენს ქმედებებს ინტერნეტ სივრცეში. არ გადაგზავნოთ (Do not forward) შეტყობინებები თქვენს კონტაქტებში არსებულ ყველა საკონტაქტო პირს;

არ გახსნათ სპამ-წერილში მითითებული ბმული, რა შინაარსისაც არ უნდა იყოს ის, ბმულზე გადასვლით შესაძლოა გადახვიდეთ საფრთხის შემცველ ვებ-გვერდზე;

გამორთეთ ავტომატური ჩამოტვირთვის ფუნქცია - სპამერები აგზავნიან HTML შეტყობინებებს, რომელსაც ბმულშივე აქვს გრაფიკული ფაილი. სპამერებს შეუძლიათ გააკონტროლონ არდესატების რეაგირება სპამ-წერილებზე. HTML-ის დეაქტივაციით კი მათ ამის შესაძლებლობას ვუზღუდავთ, შესაბამისად თავიდან ვიცილებთ ამ საკითხთან დაკავშირებულ პრობლემებს;

გამოიყენეთ ფილტრი - საფოსტო ყუთის ძრავები (მაგ: Gmail, Yahoo) გვთავაზობენ ფილტრის გამოყენებას, რომელიც ბლოკავს შეტყობინების მიღებას გარკვეული ადრესატებისგან. ასეთი ფილტრის გამოყენება ჩვენს ფოსტას უფრო დაცულს ხდის.

დანართი 15

ვირუსების (Virus), ჭიებისა (Worm) და ტროიანისგან (Trojan) თავდაცვა

როგორ მივხვდეთ, რომ ჩვენი კომპიუტერი დაინფიცირებულია?

სამწუხაროდ, არ არსებობს რაიმე კონკრეტული და ზუსტი სიმტომები (იშვიათი გამონაკლისის გარდა), რაც მიგვახვედრებს, რომ კომპიუტერი მავნე პროგრამული უზრუნველყოფითაა დაინფიცირებული. ზოგიერთ ვირუსს შეუძლია სრულიად გაანადგუროს კომპიუტერში არსებული ფაილები, ზოგიერთი კი მხოლოდ ნაწილობრივ ზღუდავს ელექტრონული მოწყობილობის გამართულ ფუნქციონირებას. ანტივირუსის არსებობა კომპიუტერში, ასევე არ არის უსაფრთხოების გარანტია, ის მხოლოდ საფრთხეების მინიმიზაციას ახდენს. თუ თქვენ იყენებთ ანტივირუსს, იგი უმეტეს შემთხვევაში მოგცემთ სიგნალს, რომელიც ვირუსის არსებობის შესახებ გაუწყებთ. ანტივირუსს შეუძლია მავნე კოდისგან ავტომატურად გაწმინდოს კომპიუტერი, თუ ეს ავტომატურად არ მოხდა მაშინ უსაფრთხოების დამატებით ზომებს უნდა მივმართოთ...

რა ვქნათ თუ ჩვენი კომპიუტერი ვირუსით დაინფიცირდა?

პირადი კომპიუტერის შემთხვევაში მიმართეთ IT სპეციალისტს, სამსახურებრივი კომპიუტერის შემთხვევაში კი - IT სამსახურს. მავნე კოდის არსებობის შემთხვევაში სპეციალისტები გაწმინდავენ კომპიუტერს და ამით ნაკლები ზარალი მოგადგებათ, როგორც თქვენს, ისე სხვა კომპიუტერებს, რომელიც იმავე ქსელშია ჩართული.

სისტემატიურად განაახლეთ ანტივირუსული პროგრამა და ხშირად გააკეთეთ კომპიუტერის სკანირება მავნე პროგრამულ უზრუნველყოფაზე. თუ თქვენს კომპიუტერზე ვერ ხერხდება ვირუსის იდენტიფიცირება და წაშლა, მაშინ სასურველია ოპერაციული სისტემა გადავაყენოთ და შემდეგ ხელახლა დავაინსტალიროთ ანტივირუსი.

რისკების შესამცირებლად გამოსაყენებელი გზები

- გამოიყენეთ ატივირუსი;
- ხშირად ცვალეთ პაროლები;
- განაახლეთ პროგრამული უზრუნველყოფა;
- დააინსტალირეთ ბრენდმაუერი;
- გამოიყენეთ ანტიჯაშუშური პროგრამები.

დანართი 16

შანტაჟის/გამოსასყიდი პროგრამა (Ransomware)

რა არის რანსომვეარი?

რანსომვეარი არის მავნე კოდი რომელსაც დამნაშავეები იყენებენ რათა დააინფიცირონ კომპიუტერი, დაშიფრონ ფაილები მყარ დისკზე და გახადონ იგი მომხმარებლისთვის მიუწვდომელი. კიბერკრიმინალის მიზანია დეშიფრაციის გასაღების სანაცვლოდ ფინანსური ანაზღაურების მიღება.

რანსომვეარის სპეციფიკა მდგომარეობს იმაში რომ, თქვენი კომპიუტერის დაინფიცირების შემდგომ ის შეეცდება გაავრცელოს მავნე კოდი სხვა დაკავშირებულ კომპიუტერებზე და სისტემებზე.

რანსომვეარის გამოყენება მზარდია. ბოლო რამდენიმე წლის განმავლობაში მსოფლიოს უდიდესი ორგანიზაციების წინააღმდეგ შეტევები რანსომვეარის გამოყენებით განხორციელდა. 2017 წელს რანსომვერის მავნე კოდებით 300,000-ზე მეტი კომპიუტერის დაინფიცირება მოხდა.

როგორ ხვდება რანსომვეარი კომპიუტერში?

ხშირ შემთხვევაში რანსომვეარი ჩვენს კომპიუტერში ხვდება ფიშინგ ელექტრონული წერილის მეშვეობით, რომელიც შენიღბულია და იგზავნება მსხვერპლისთვის ცნობადი ლეგიტიმური ორგანიზაციიდან ან მისთვის ნაცნობი ადამიანისგან. შესაბამისად მსხვერპლი ხშირ შემთხვევაში დაუფიქრებლად ხსნის ელექტრონულ წერილზე მიმაგრებულ ფაილს რომელიც შეიცავს მავნე კოდს.

რა შეიძლება გავაკეთო რათა არ დაუშვა რანსომვეარით კომპიუტერის დაინფიცირება

- დავაკვირდეთ მიღებულ ელექტრონულ წერილში მიმაგრებულ ფაილებს.

მიუხედავად იმისა, რომ გამომგზავნის ვინაობა ჩვენთვის ცნობილია, გამოვიჩინოთ სიფრთხილე მეილზე მიმაგრებული ფაილების გახსნის დროს. განსაკუთრებით როცა ვხსნით zip ფაილს.

- დავაკვირდეთ გამომგზავნის ელექტრონული ფოსტის მისამართს.
- გამოვიჩინოთ სიფრთხილე ბმულებზე გადასვლისას. მივაქციოთ ყურადგება ვებგდვერდის მისამართს. ხშირ შემთხვევაში ბოროტმოქმედები იყენებენ ლეგიტიმური ვებგვერდების იდენტურ ვებგვერდებს, მცირედი განსხვავებით ვებგვერდის მისამართში ან დომეინში. მაგალითად, .COM მაგივრად .NET
- გამოვიყენოთ ლიცენზირებული პროდუქტები, ანტივირუსები და ფაიერვოლები.

დანართი 17

ჯაშუში პროგრამა (Spyware)

რა არის ჯაშუში პროგრამა?

ჯაშუში პროგრამები იპარავენ ჩვენს პირად მონაცემებს, წვდომას ახდენენ ფაილებსა თუ პაროლებზე, იმახსოვრებენ ჩვენს პაროლებს ან კიდევ უარესი წვდომას იღებენ მთლიანად ჩვენს კომპიუტერზე, ვებ კამერაზე, მიკროფონზე თუ სამუშაო დაფაზე.

ჯაშუშური პროგრამა თქვენს წინააღმდეგ შესაძლოა, ისე გამოიყენებოდეს, რომ თქვენ, ამის შესახებ ვერაფერი შეიტყოთ. არის შემთხვევები, როდესაც პროგრამა რამდენიმე სიმპტომს იძლევა. მაგალითად, კომპიუტერული მოწყობილობა, მათ შორის ტელეფონი, შესაძლოა შენელებულად მუშაობდეს, და "იჭედებოდეს". ჩნდება კითხვები:

- რა ტიპის ინფორმაციის შეგროვება ხდება?
- ვინ იღებს ამ ინფორმაციას?
- როგორ გამოიყენება ეს ინფორმაცია?

როგორ მივხვდეთ რომ ჩვენს კომპიუტერში ჯაშუში პროგრამაა?

- თქვენ მუდმივად გიხტებათ „Pop Up" ფანჯრები;
- თქვენი გადამისამართება ხდება სხვადასხვა ვებ გვერდებზე;
- თქვენს ბრაუზერში ახალი პანელები ჩნდება;
- თქვენი ბრაუზერის მთავარი გვერდი მოულოდნელად თავისით იცვლება;
- წამდაუწუმ ჩნდება ვინდოუსის „error" შეტყობინებები;
- თქვენი კომპიუტერი ნელა მუშაობს და დიდ დროს ანდომებს მარტივი ოპერაციების ჩატარებას;

როგორ დავიცვათ თავი, რომ პროგრამამ ვერ მოახერხოს ჩვენს კომპიუტერზე დაინსტალირება

იმისთვის რომ შემთხვევით ჩვენ თვითონ არ შევუწყოთ ხელი ასეთი პროგრამის ჩვენს ელექტრონულ მოწყობილობაზე დაინსტალირებას უნდა გავითვალისწინოთ შემდეგი რჩევები:

- არ დააკლიკოთ „Pop Up" ფანჯრებს- ხშირ შემთხვევაში ასეთი ფანჯრები ჯაშუში პროგრამის პროდუქტია და მასზე დაკლიკებით ჩვენ თვითონ ვაინსტალირებთ პროგრამას ჩვენს კომპიუტერზე
- დახურეთ მოულოდნელად წამოწყებული დიალოგის ფანჯრები- სიფრთხილე გამოიჩინეთ როდესაც რაიმე პროგრამის ან რაიმე დავალების განხორციელებისთვის თანხმობას გთხოვენ და არ დაეთანხმოთ მათ;
- მოერიდეთ უფასოდ ჩამოტვირთვად პროგრამულ უზრუნველყოფას;

- არ გადახვიდეთ ელექტრონულ ფოსტაზე მიღებული შეტყობინების ლინკზე, რომელიც ვითომდა ანტიჯაშუშურ პროგრამულ უზრუნველყოფას გთავაზობთ.

როგორ გავთავისუფლდეთ ჯაშუში პროგრამისგან?

- ანტივირუსით მოახდინეთ კომპიუტერის სკანირება- ზოგ ანტივირუსულ პროგრამას შეუძლია აღმოაჩინოს და გაანადგუროს ჯაშუში პროგრამა;
- აამოქმედეთ ლეგიტიმური პროგრამა რომელიც გათვლილია ჯაშუში პროგრამის მოშორებაზე;
- დარწმუნდით რომ თქვენი ანტივირუსული პროგრამა და ანტიჯაშუშური პროგრამული უზრუნველყოფა ერთმანეთთან თავსებადია