პერსონალურ კომპიუტერში ძირითადად მოიაზრება ლეპტოპები და დესკტოპ კომპიუტერები. ისინი იყენებენ ოპერაციულ სისტემებს, როგორებიცაა Windows, MacOS, Linux და სხვა. მათგან ყველაზე გავრცელებულია Microsoft-ის მიერ წარმოებული Windows. მიუხედავად იმისა, რომ უახლესი თაობის ოპერაციული სისტემები საკმაოდ დაცულია, არის საკითხები, რომლებიც უშუალოდ მომხმარებელზეა დამოკიდებული.

პერსონალური კომპიუტერის უსაფრთხოების მნიშვნელობა

ყოველდღიურად მუშაობის პროცესში უამრავი პროგრამის და აპლიკაციის გამოყენება გვიწევს. არაოფიციალური ვებგვერდებიდან პროგრამული უზრუნველყოფის გადმოწერა უსაფრთხოების რისკებთანაა დაკავშირებული და ისინი სერიოზული საფრთხის ქვეშ აყენებს თქვენს კომპიუტერზე შენახულ პერსონალურ ინფორმაციას. ერთი მავნე პროგრამის გადმოწერაც კი საკმარისია კიბერდამნაშავისთვის, რომ წვდომა მოიპოვოს თქვენს სისტემაზე, მოწყობილობის მიკროფონზე და კამერაზე; მოიპაროს წლების განმავლობაში შენახული ფაილები, სამსახურეობრივი დოკუმენტები ან/და სამუდამოდ შეგიზღუდოთ მათზე წვდომა; ხელში ჩაიგდოს სენსიტიური მასალები და სცადოს თქვენი დაშანტაჟება; აღმოაჩინოს კომპიუტერში შენახული პაროლები, ციფრული ანგარიშების მონაცემები, საბანკო რეკვიზიტები და გამოიყენოს არაკანონიერი საქმიანობისთვის; დააინფიციროს ქსელში ჩართული სხვა მოწყობილობები, განსაკუთრებით სამუშაო გარემოში თანამშრომლების კომპიუტერები და ორგანიზაციის სერვერები; გამოიყენოს თქვენი მოწყობილობა „შუამავლად“, განახორციელოს შეტევები სხვა ობიექტებზე თქვენი კომპიუტერის გავლით და ამგვარად შეცდომაში შეიყვანოს სამართალდამცავები.

პროგრამები და ოპერაციული სისტემა

პერსონალურ კომპიუტერში ნებისმიერი პროგრამის ინსტალაციამდე აუცილებელია მოიძიოთ საკმარისი ინფორმაცია და დარწმუნდეთ, რომ წყარო, რომელსაც აპლიკაციის გადმოსაწერად იყენებთ, არის ოფიციალური და აქვს მაღალი რეპუტაცია. განსაკუთრებით ხშირია პირატული პროგრამების გამოყენება. ასეთი პროგრამები, ცხადია, ოფიციალურ ვებგვერდებზე არ გვხვდება და მათი უცხო წყაროებიდან გადმოწერა უსაფრთხოების მაღალ რისკებთანაა დაკავშირებული. აღსანიშნავია, რომ თუნდაც სანდო პროგრამის ერთჯერადად დაყენება არ არის საკმარისი იმისათვის, რომ მისი უსაფრთხოდ გამოყენება შეძლოთ. რეგულარული განახლება არანაკლებ მნიშვნელოვანი და აუცილებელია. მათი საშუალებით ხდება მოძველებული კოდის შეცვლა, ახალი ფუნქციონალის დამატება, ხარვეზების გამოსწორება და მოწყვლადობების აღმოფხვრა. უმეტეს შემთხვევაში პროგრამებს აქვთ ჩაშენებული ხელსაწყო, რომელიც ავტომატურად ანახლებს ან გთავაზობთ განახლების პროცესის დაწყებას, რაც მომხმარებლისთვის კომფორტული და მოსახერხებელია. ზოგიერთი პროგრამისთვის კი საჭიროა, თავად გადაამოწმოთ ოფიციალურ ვებგვერდზე გამოქვეყნებული განახლებები.

პროგრამებთან ერთად, განახლებული ოპერაციული სისტემაც გაცილებით მდგრადი და დაცულია კიბერდამნაშავეების წინაშე. როგორც წესი Windows-ის სისტემა დროდადრო ავტომატურად გთავაზობთ განახლების დაყენებას, თუმცა მისი შემოწმება თავადაც შეგიძლიათ. ამისათვის საჭიროა გახსნათ Start menu, ჩაწეროთ „Check for updates” და დააჭიროთ პირველ ბმულს, რომელიც პარამეტრების შესაბამის სექციას გახსნის. „Check for updates" ღილაკზე დაჭერით სისტემა შეამოწმებს და დაიწყებს განახლების პროცესს.

აღსანიშნავია, რომ ძველი სისტემები, როგორიცაა Windows 7, Windows 8/8.1 და მათი წინამორბედები აღარ იღებენ რეგულარულ განახლებებს Microsoft-ის მხრიდან, შესაბამისად მათი გამოყენება უსაფრთხოების რისკების გამო არ არის მიზანშეწონილი.

MacOS-ის შემთხვევაში, სისტემის განახლების შესამოწმებლად დააჭირეთ System settings, აირჩიეთ General და გახსენით Software Update.

ანტივირუსი

მიუხედავად იმისა, თუ რა სიფრთხილით ეკიდებით ახალი პროგრამების გადმოწერას, შანსი იმისა, რომ თქვენს პერსონალურ კომპიუტერში მავნე კოდი აღმოჩნდება, მაინც არსებობს. მსგავსი საფრთხისგან თავის დასაცავად შეგიძლიათ გამოიყენოთ ანტივირუსი - სპეციალურად შექმნილი პროგრამული უზრუნველყოფა, რომლის დანიშნულება არის სისტემაში შემოჭრილი საეჭვო ფაილების აღმოჩენა, მონიტორინგი და საჭიროების შემთხვევაში მათი წაშლა. მსგავსი ფაილები შეიცავენ მავნე კოდს, რომელსაც პოტენციურად შეუძლია თქვენი პერსონალური მონაცემების მოპარვა, დაშიფრვა ან განადგურება. ამიტომ მნიშვნელოვანია შეარჩიოთ ძლიერი, ხარისხიანი და მაღალი რეპუტაციის მქონე ანტივირუსი და მოარგოთ თქვენს საჭიროებებსა და მოთხოვნებს.

კომერციული ანტივირუსი:

Bitdefender Antivirus Plus;

Norton 360;

Avast Premium Security;

McAfee Total Protection;

Trend Micro Antivirus+ Security.

უფასო ანტივირუსი:

Bitdefender;

TotalAV;

Norton;

McAfee;

Avast.

Windows Defender არის Microsoft-ის მიერ წარმოებული ანტივირუსი, რომელიც Windows-სისტემებს მოყვება და გარკვეულ დონეზე იცავს მომხმარებელს მავნე კოდებისგან. მას აქვს უნარი, რეალურ დროში დააკვირდეს სისტემაში მიმდინარე პროცესებს, დაასკანეროს ფაილები და აღმოაჩინოს საეჭვო აქტივობები. სამართავ პანელზე გადასასვლელად Start მენიუში უნდა ჩაწეროთ და გახსნათ Windows Security. თქვენ დაინახავთ აპლიკაციის რეკომენდაციებს და შესაბამის ღილაკებს.

აღსანიშნავია, რომ კიბერდამნაშავეებისთვის Windows Defender-ის გვერდის ავლა არ წარმოადგენს განსაკუთრებულ სირთულეს. გაზრდილი უსაფრთხოების ზომების მისაღებად შეგიძლიათ სხვა, შედარებით ძლიერი, ფასიანი ანტივირუსების გამოყენება.

თუ ეჭვი გაქვთ, რომ თქვენი კომპიუტერი დაინფიცირებულია მავნე კოდით, განაახლეთ ანტივირუსი და დაასკანერეთ თქვენი მოწყობილობა, წაშალეთ საეჭვო პროგრამები. შეცვალეთ თქვენი პაროლები და ფინანსური თაღლითობის შემთხვევაში მიმართეთ ბანკის წარმომადგენელს. თუ ინციდენტი სამსახურში შეგემთხვათ, დაუყოვნებლივ შეატყობინეთ ტექნიკური დახმარების ჯგუფს რომ მათ დროულად შეძლონ მომხდარ ინციდენტზე რეაგირება.

ავთენტიფიკაცია და დაბლოკვა

პერსონალური კომპიუტერის გამოსაყენებლად საჭიროა შექმნათ ანგარიში და აირჩიოთ ავთენტიფიკაციის მეთოდი (ავთენტიფიკაციის მეთოდებზე დეტალური ინფორმაცია იხილეთ მე-3 თავში). ამგვარად კომპიუტერში შენახულ თქვენს პერსონალურ ინფორმაციაზე მხოლოდ თქვენ გექნებათ წვდომა, შესაბამისად სისტემის ყოველი ჩატვირთვისას მოგიწევთ დაადასტუროთ თქვენი ვინაობა. თუ ავთენტიფიკაციის მეთოდად იყენებთ პინ კოდს ან პაროლს, რეკომენდებულია მათი პერიოდული შეცვლა. ამისათვის Start მენიუს დახმარებით უნდა გახსნათ sign-in options პარამეტრები და დააყენოთ ახალი და უნიკალური პაროლი/პინ კოდი.

ასევე, მნიშვნელოვანია შემდეგი ჩვევის გამომუშავება - სამუშაო ადგილის დატოვებამდე აუცილებლად უნდა დაბლოკოთ პერსონალური კომპიუტერი (გამოხვიდეთ პირადი ანგარიშიდან). ამისთვის საჭიროა, გამოიყენოთ კლავიატურის კომბინაცია Windows+L.

მყარი დისკის შიფრაცია

პერსონალური კომპიუტერის დაკარგვის შემთხვევაში, მიუხედავად იმისა რომელ ავთენტიფიკაციის მეთოდს გამოიყენებთ, კიბერდამნაშავეს შეუძლია მყარი დისკის გახსნა და თქვენს პერსონალურ ინფორმაციაზე წვდომის მოპოვება. ამ პრობლემის მოგვარება შესაძლებელია მყარი დისკის დაშიფვრით.

BitLocker არის Windows-ის სისტემებში ჩაშენებული ხელსაწყო, რომელიც საშუალებას გაძლევთ სისტემის გათიშვის ან გადატვირთვის დროს ავტომატურად დაშიფროთ მყარ დისკზე მოთავსებული მონაცემები, მათი დეშიფრაციისთვის კი გამოიყენოთ პაროლი ან ავთენტიფიკაციის სხვა მეთოდი. გაითვალისწინეთ, რომ BitLocker-ის სრული ფუნქციონალის გამოსაყენებლად საჭიროა Windows-ის Pro ვერსია. ჩასართავად Start მენიუში აკრიფეთ „BitLocker“ და გახსენით შესაბამისი პარამეტრები. სამართავ პანელზე დააჭირეთ ღილაკს „Turn on BitLocker” და მიყევით ინსტრუქციას.

აღსანიშნავია, რომ კომპიუტერის ჩართვისა და ავთენტიფიკაციის შემდეგ მონაცემები დაშიფრულ მდგომარეობაში რჩება. მათი შიფრაცია და დეშიფრაცია ხდება ჩაწერის და წაკითხვის მომენტში.

FileVault არის MacOS-ის სისტემებში ჩაშენებული ხელსაწყო, რომელიც საშუალებას გაძლევთ სისტემის გათიშვის ან გადატვირთვის დროს ავტომატურად დაშიფროთ მყარ დისკზე მოთავსებული მონაცემები. თუ ელექტრონულ მოწყობილობას აქვს „Apple silicon“ ან „Apple T2 Security Chip“-ი, FileVault ავტომატურად ირთვება, დანარჩენ შემთხვევაში კი ხელსაწყოს ჩართვა იქნება საჭირო. ჩასართავად Start მენიუში გადადით System Settings>Privacy&Security>FileVault და დააჭირეთ ღილაკს „Turn on” და მიყევით ინსტრუქციას.

საფრთხის შემცველი USB მოწყობილობები

ინტერნეტთან ერთად პერსონალურ კომპიუტერში მავნე კოდის შემოღწევის კიდევ ერთი გზა USB მოწყობილობებია. USB Baiting არის სოციალური ინჟინერიის ერთ-ერთი ფორმა სადაც კიბერდამნაშავე განზრახ ტოვებს მავნე კოდით დაინფიცირებულ USB მეხსიერების ბარათებს სამიზნე დაწესებულების ან პიროვნების ტერიტორიაზე მაგ. პარკინგზე, სადარბაზოში და ა.შ. იმ იმედით რომ სამიზნე პიროვნება აიღებს გარე მეხსიერების ბარათს და შეაერთებს თავის ელექტრონულ მოწყობილობაზე. მავნე კოდით დაინფიცირებული USB მეხსიერების ბარათის დაერთებით კი კიბერდამნაშავე მოიპოვებს წვდომას ელექტრონულ მოწყობილობაზე. ამიტომ მნიშვნელოვანია, რომ კომპიუტერში USB მეხსიერების შეერთებამდე მის სანდოობაში დარწმუნდეთ. მეტი უსაფრთხოებისთვის პარალელურად გამოიყენეთ ანტივირუსიც.

Backup - სარეზერვო ასლი

Backup გულისხმობს ციფრული მონაცემების ასლების შექმნასა და მათ შენახვას დამატებით გამოყოფილ, განცალკევებულ მოწყობილობაზე. სარეზერვო ასლების მთავარი დანიშნულება მონაცემების დაკარგვის რისკის შემცირებაა. დაკარგვის მიზეზი შეიძლება იყოს მოწყობილობის ფიზიკური დაზიანება, პროგრამული უზრუნველყოფის გაუმართაობა, შემთხვევით წაშლა, კიბერშეტევა, ბუნებრივი კატასტროფა და სხვა.

სარეზერვო ასლების შენახვის სხვადასხვა მეთოდი არსებობს. მათ შორისაა დამატებითი მეხსიერების ბარათის გამოყენება და პერიოდულად ფაილების ხელით გადატანა. შედარებით მეტად მოსახერხებელია ღრუბლოვანი ტექნოლოგიების გამოყენება, როგორებიცაა Dropbox, OneDrive. (იხ. ვრცლად მე-8 თავში)

ძლიერი პაროლის მნიშვნელობა

დღესდღეობით პაროლი ერთ-ერთი ყველაზე გავრცელებული მექანიმზია ციფრულ სივრცეში ავთენთიფიკაციისთვის. ვინაიდან ანგარიშები პაროლებითაა დაცული, თუ თავდამსხმელი თქვენს პაროლს მოიპოვებს, წვდომა ექნება ყველა იმ ინფორმაციასთან, რაც თქვენს ანგარიშზეა. შემადგენლობის მიხედვით პაროლი შესაძლოა იყოს ძლიერი და სუსტი. სუსტისგან განსხვავებით, ძლიერი პაროლი კომპლექსურია და შედგება როგორც დიდი და პატარა ასოებისგან, ასევე სხვადასხვა ციფრებისა და სიმბოლოებისგანაც. მიუხედავად მსოფლიოში გავრცელებული თავდასხმებისა, მილიონობით ადამიანი დღემდე იყენებს ერთიდაიგივე მარტივ პაროლს სხვადასხვა ანგარიშისთვის, რაც ძალიან დიდი საფრთხეა მათი გატეხვის სიმარტივის გათვალისწინებით. მაგალითად, თუ თავდამსხმელმა მოახერხა და ერთ-ერთი მომხმარებლის სოციალური ქსელის ანგარიშის პაროლი გატეხა და იმავე მომხმარებელს ელექტრონულ მეილზეც ზუსტად იგივე პაროლი უყენია, ამ შემთხვევაში შესაძლოა ჰაკერმა ორივე პლატფორმის ანგარიში ჩაიგდოს ხელში.

ყველაზე გავრცელებული პაროლებზე თავდასხმის გზებია:

Brute Force Attacks - არის პაროლებზე თავდასხმის ერთ-ერთი გზა, როდესაც თავდამსხმელი ცდილობს თითოეული სიმბოლოს, ციფრისა და ასოს გამოყენებით დააგენერიროს სხვადასხვა ვარიანტები და ეცადოს თითოელი ვარიანტი მოარგოს რეალურ პაროლს. მაგალითად თუ პაროლი შედგება ლათინური ალფაბეტის 3 პატარა ასოსგან (a,b,c) მაშინ პაროლების შესაძლო მნიშვნელობები იქნებოდა:

aaa, aab, aac, aba, abb, abc, aca, acb, acc, baa, bab, bac, bba, bbb, bbc, bca, bcb, bcc, caa, cab, cac, cba, cbb, cbc, cca, ccb, ccc

Dictionary Attacks - გულისხმობს უკვე არსებული პაროლების ბაზების გამოყენებას რეალურის გამოცნობის მიზნით. მაგალითად, თუ ცნობილია მომხმარებლის სახელი და მიზანი მისი პაროლის გატეხვაა, შესაძლებელია საჯაროდ არსებული პაროლების სიების გამოყენება და ერთ კონკრეტულ მომხმარებლის სახელზე მორგება, მაგალითად 1 მილიონი შესაძლო პაროლი რომელიც სიის სახით ერთ ფაილში ინახება.

Pass-the-Hash Attacks - გულისხმობს ისეთ თავდასხმას, სადაც სუსტი კონფიგურაციისას თავდამსხმელს არ სჭირდება უშუალო პაროლის ცოდნა და ავტორიზაციის გავლა შეუძლია მომხმარებლის პაროლის ჰეშით, რომელიც ასევე არაკანონიერი გზით აქვს მოპოვებული. ეს ჰეში შესაძლოა გამოიყურებოდეს შემდგნაირად "8846F7EAEE8FB117AD06BDD830B7586C", რაც გაშიფრვის შედეგად გვაძლევს "password" სიტყვას.

იმისთვის, რომ თქვენი ანგარიშები იყოს მეტად დაცული, უნდა იცოდეთ თუ რა საფრთხეები არსებობს მათზე წვდომის მოსაპოვებლად:

დაუშიფრავი ვებსაიტიდან შეყვანილი ინფორმაციის მოპარვა;

ყურადღებით უნდა ვიყოთ დაუშიფრავი (http) ვებსაიტების გამოყენებისას ანგარიშის სახელებისა და პაროლების მითითებისას, რადგან ამ დროს ჩვენ მიერ შეყვენილი ნებისმიერი ინფორმაცია დაუშიფრავად მოძრაობს ქსელში და Person in the Middle თავდასხმის შემთხვევაში, შესაძლებელი იქნება უცხო პირის მიერ მათი ნახვა.

პაროლის გამოცნობა;

პაროლი არ უნდა იყოს ძალიან მარტივი ან ინდივიდუალური პიროვნებისთვის დამახასიათებელი, მაგალითად თუ თქვენი პაროლი შედგება თქვენივე სახელისა და დაბათების თარიღის კომბინაციისგან მაშინ მარტივი იქნება მისი გამოცნობა.

პაროლის შემცველი ფაილის მოპარვა;

ხშირად ადამიანები პაროლებს ტექსტურ დოკუმენტში ინახავენ და თვალსაჩინოდ უდევთ კომპიუტერში, იმ შემთხვევაში თუ თქვენი მოწყობილობა დავირუსდა მავნე ფაილით, შესაძლებელია თქვენი შენახული პაროლი თავდამსხმელმა მოიპაროს და სხვადასხვა პლატფორმაზე შესასვლელად გამოიყენოს.

პაროლის აღდგენის მეშვეობით მისი განულება;

ზოგიერთ პლატფორმაზე პაროლის შექმნისას ხშირია 3 დამატებითი კითხვა პირად ინფორმაციასთან დაკავშირებით. შესაძლოა იყოს დაბადების ადგილი, ბავშობის მეტსახელი, ან დედის სახელი. ამ შემთხვევაში მარტივია ამგვარ კითხვებზე პასუხის მოძიება სხვადასხვა სოციალური ქსელიდან რაც შესაძლოა გამოყენებულ იქნას სხვადასხვა მომხმარებლის პაროლის გასანულებლად.

მოტყუებით გამოძალვა;

მოტყუებით გამოძალვის ერთ-ერთი ყველაზე გავრცელებული მაგალითია ფიშინგი. ასევე შესაძლოა სოციალურ ქსელში ვინმემ შთაბეჭდილება მოახდინოს თქვენზე, დაგიმეგობრდეთ და შემდგომ იმდენად მოიპოვოს თქვენი ნდობა რომ პაროლიც გამოგტყუოთ ან თუნდაც ახლობელ ადამიანად გაგაცნოთ თავი. ყურადღებით იყავით და არავის გაუზიაროთ თქვენი პაროლი.

სუსტი პაროლის გატეხვა.

სუსტი პაროლის შემთხვევაში, მაგალითად "123456", სხვადასხვა ხელსაწყოთი შესაძლებელია წამებში გატეხონ თქვენი პაროლი. სწორედ ამიტომ უნდა გამოვიყენოთ ძლიერი და კომპლექსური პაროლები.

საბოლოოდ, მნიშვნელოვანია, თქვენი ანგარიშების დასაცავად გამოიყენოთ კომპლექსური პაროლები. პაროლი კომპლექსურია, როდესაც იგი შედგება დიდი და პატარა ასოებისგან, ციფრებისა და სიმბოლოებისგან. საერთაშორისოდ აღიარებული პრაქტიკის თანახმად, პაროლები, რომლის სიგრძეა 12-დან 25 სიმბოლომდე, ნაკლებად მოწყვლადია ჰაკერებისთვის.

კომპლექსური პაროლის შექმნა შესაძლებელია:

დამოუკიდებლად, შემთხვევითი სიმბოლოების მოფიქრებით;

პაროლების მენეჯერის დახმარებით.

ზოგადად პაროლი უნდა იყოს რთულად გამოცნობადი. მარტივად რომ ვთქვათ, სპეციალურ ხელსაწყოებს მათ გასატეხად ძალიან დიდი დრო უნდა სჭირდებოდეს; უფრო მეტიც - იმდენად დიდი, რომ ბოროტმოქმედი საბოლოოდ უარს ამბობდეს პაროლის გამოცნობაზე.

პაროლების მენეჯმენტი

პაროლების მენეჯერი არის ერთგვარი საცავი, სეიფი სადაც შეგიძლიათ შეინახოთ თქვენთვის სასურველი პაროლები. იმ შემთხვევაში, თუ ბევრ სხვადასხვა ანგარიშს იყენებთ

სხვადასხვა პლატფორმაზე, ყველა პაროლის დამახსოვრება არ მოგიწევთ. საჭირო იქნება მხოლოდ ერთი, მთავარი სეიფის გასაღების დამახსოვრება, სადაც შენახული გექნებათ თქვენს ანგარიშებზე ინფორმაცია. სწორედ პაროლების მენეჯერია ყველაზე ოპტიმალური მიდგომა ბევრ ანგარიშთან გასამკლავებლად.

რას აკეთებს პაროლების მენეჯერი?

ინახავს თქვენი ანგარიშების მონაცემებს — დღესდღეობით უამრავ ადამიანს აქვს ათობით სხვადასხვა ციფრული ანგარიში. თითოეული მათგანის მონაცემების (მომხმარებლის სახელები, ელფოსტის მისამართების და პაროლები) ფურცელზე ჩამოწერა, ან კომპიუტერში ლოკალურად შენახვა საფრთხის შემცველია. ამ შემთხვევაში პაროლების მენეჯერი ამარტივებს საქმეს და ინახავს ყველა ანგარიშის მონაცემს უსაფრთხოდ. ძირითად შემთხვევაში პაროლების მენეჯერებს დამატებით დაცვა აქვთ უსაფრთხოების თვალსაზრისით, თუმცა უმჯობესია, აქაც მთავარ გასაღებზე დაემატოს ორმაგი ავტორიზაცია.

ქმნის ძლიერ, უნიკალურ პაროლებს — პაროლების მენეჯერი საშუალებას გაძლევთ დააგენერიროთ თქვენთვის სასურველი შემცველობის და სირთულის პაროლი. მისი წყალობით ყველა ანგარიშზე უნიკალური პაროლი გექნებათ.

პაროლების მენეჯერი შეგიძლიათ მოარგოთ თქვენს საჭიროებებსა და მოთხოვნებს. არსებობს რამდენიმე საიმედო და უსაფრთხო ვერსია. კომერციული პაროლების მენეჯერი:

Dashlane;

1Password;

Keeper;

NordPass.

უფასო პაროლების მენეჯერი:

KeePass;

BitWarden;

LastPass;

Norton.

ზოგიერთი კომერციული პაროლების მენეჯერი მომხმარებელს სთავაზობს უფასო სერვისს, იმ შემთხვევაში თუ პაროლების შენახვის გარდა დამატებითი ფუნქციები არ სჭირდებათ.

პაროლების მენეჯერი იყოფა ორ კატეგორიად, იმის მიხედვით, თუ სად ინახავენ მომხმარებლების ანგარიშების მონაცემებს.

პირველი კატეგორია მომხმარებლის ანგარიშების მონაცემებს ინახავს ლოკალურად უშუალოდ მოწყობილობაზე. მაგალითად უფასო პაროლების მენეჯერი KeePass თქვენს

მოწყობილობაზე ინახავს პაროლებს, ეს კი უფრო მეტად უზრუნველყოფს კონფიდენციალურობას, ვინაიდან ინტერნეტ სივრცეში არ ინახება ისინი. რა თქმა უნდა, უსაფრთხოების დონე იზრდება, მაგრამ ამისთვის საჭიროა გამოყენების წესებისა და კიბერჰიგიენის ცოდნა.

მეორე კატეგორია ღრუბლოვან ტექნოლოგიას შეეხება. არსებობს პაროლების მენეჯერები, რომლებიც მომხმარებლის ანგარიშების შესახებ ინფორმაცია ღრუბლოვან სისტემაში (Cloud) ინახავენ. ამით მომხმარებელს უმარტივდება ანგარიშებზე წვდომა, რამდენადაც სინქრონიზაციის საშუალებით აღნიშნული ინფორმაცია სხვადასხვა მოწყობილობაზე ხდება ხელმისაწვდომი. ერთადერთი მინუსი სხვისი ინფრასტრუქტურაა, ვინაიდან ღრუბლოვანი ტექნოლოგიაა გამოყენებული და არა ლოკალური მოწყობილობა.

მულტიფაქტორული ავთენტიფიკაცია-MFA (Multi-Factor Authentication)

მულტიფაქტორული ავთენტიფიკაცია არის ფუნქცია, რომელიც დაცვის დამატებითი მექანიზმია ანგარიშებზე. იმ შემთხვევაში, თუ თავდამსხმელებმა შეძლეს პაროლების ხელში ჩაგდება, მულტიფაქტორული ავთენტიფიკაცია საშუალებას არ მიცემს მათ, მოიპოვონ წვდომა ანგარიშებზე.

სამწუხაროდ, ყველაზე ძლიერი პაროლიც კი ბოლომდე ვერ დაიგიცავთ. ჰაკერებს შეუძლიათ უშუალოდ პლატფორმებიდან მოიპარონ ანგარიშების შესახებ ინფორმაცია. აღნიშნული ხშირად ხდება, როცა პოპულარულ, ცნობილ საიტებს ტეხავენ. ამას გარდა შესაძლოა ინტერნეტ სივრციდან შემთხვევით გადმოწეროთ რაიმე სახის ვირუსი, ან მავნე კოდი, რომელიც თქვენი მომხმარებლის სახელსა და პაროლს იპარავს. სწორედ ამ დროს ერთვება საქმეში ორმაგი ავთენტიფიკაცია დამატებითი დაცვის მექანიზმად, რომელიც თავდამსხმელს მოპარული პაროლის გამოყენების მიუხედავად არ აძლევს ანგარიშზე შესვლის საშუალებას. აქედან გამომდინარე, საჭიროა ორმაგი ავთენტიფიკაციის (2FA) გამოყენება თქვენი ციფრული ანგარიშების დასაცავად. ეს იმას ნიშნავს, რომ პაროლის შეყვანის გარდა (პირველი ფაქტორი), თქვენ კვლავ უნდა გააგზავნოთ მეორე ტიპის ინფორმაცია (მეორე ფაქტორი) ავტორიზებული წვდომისთვის.

რა შეიძლება იყოს ავტორიზაციის მეორე ფაქტორი?

ციფრული ანგარიშების უმეტესობა მომხმარებლებს საშუალებას აძლევს აირჩიონ ვერიფიკაციის სამი სხვადასხვა ფაქტორიდან ერთ-ერთი:

“რაიმე, რაც იცი” (Something you know) - მაგ. PIN-კოდი, დამატებითი პაროლი, ან რამდენიმე უსაფრთხოების კითხვაზე პასუხი.

“რაიმე, რაც გაქვს” (Something you have) - ფიზიკური მოწყობილობა - Smart Card (პროგრამული უზრუნველყოფის პატარა მოწყობილობა) ან თქვენი სმარტფონი, რომელიც შეიძლება გამოიყენოთ ვერიფიკაციის კოდების მისაღებად, მოკლე ტექსტური შეტყობინებით ან სპეციალური აპლიკაციების საშუალებით.

“რაიმე, რაც ხარ” (Something you are) - თქვენი სხეულის ნაწილი: თითის ანაბეჭდი, სახე ან თვალის ბადურა და ა.შ.

ჩამოთვლილთაგან ყველაზე მეტად დაცული არის **“რაიმე, რაც ხარ” (Something you are),** ვინაიდან თითი ანაბეჭდის, თვალის ან სახის სკანირების გაყალბება უფრო რთულია, ვიდრე PIN-ის ან ფიზიკური ბარათის.

ორმაგი ავთენტიფიკაციის გამოყენების დროს თქვენი ანგარიშები დაცულია, მაშინაც კი, როდესაც თქვენი პაროლები გატეხილია.

პაროლების უსაფრთხოების საუკეთესო პრაქტიკა

უპირველესად, აუცილებელია თითოეულ ანგარიშზე გვქონდეს უნიკალური პაროლი. ერთნაირი პაროლების გამოყენებისას დიდია შანსი, რომ თუ ერთი კონკრეტული პლატფორმის ანგარიშს დაეუფლნენ, შემდგომ მარტივად შეეძლებათ სხვა პლატფორმებსა და ანგარიშებზე გადასვლაც. თუ ყველაფერზე ერთი და იმავე პაროლს გამოვიყენებთ, ამით დიდი საფრთხე შეიქმნება როგორც პირად ანგარიშებზე, ასევე სამსახურეობრივ ინფორმაციასაც და შესაბამისად თავად სამუშაო ადგილსაც/კორპორაციას.

ერთი და იმავე პაროლის სხვადასხვა პლატფორმაზე გამოყენება დაუშვებელია, რადგან ერთი ჰეშირების ალგორითმის შემთხვევაში (იმ შემთხვევაში თუ საიტი, რომელსაც იყენებთ უზრუნველოყოფს პაროლის დაშიფრვას) მიიღება ერთნაირი ჰეშები, რაც ამ პაროლების გატეხვის ალბათობას ზრდის.

ხშირია შემთხვევა, როცა ანგარიშების შექმნის შემდგომ მომხმარებლებს ავიწყდებათ ავტორიზაციისთვის საჭირო ინფორმაცია ან აღარ სჭირდებათ. დიდია ალბათობა იმის, რომ რამდენიმე წლის წინანდელი ანგარიში ან თავად საიტი გატყდეს და ასეთი მონაცემები მოიპარონ. ამიტომაც, მნიშვნელოვანია ყველა პლატფორმისთვის სხვა ყველა რეკომენდაციასთან ერთად უნიკალური პაროლის დაყენება.

დროდადრო ჰაკერები უამრავ საიტს ტეხავენ და მონაცემთა ბაზებში არსებულ ანგარიშის სახელებსა და პაროლებს იპარავენ. ამ შემთხვევაში საიტის მომხმარებელს არანაირი ბერკეტი გააჩნია, გარდა პაროლის შეცვლისა და ორმაგი ავთენტიფიკაციის გამოყენებისა. ასეთი თავდასხმების შედეგად მოპოვებულ პაროლებს გაჟონილი პაროლები ჰქვიათ და ისინი მილიარდობითაა.

თუ გსურთ დარწმუნდეთ, რომ თქვენი ანგარიშის ელფოსტის მისამართი არცერთ გაჟონილ ბაზაში მოხვედრილა, შეგიძლიათ, გადაამოწმოთ შემდეგ საიტზე
- **https://haveibeenpwned.com/**

პაროლების გადამოწმების შემთხვევაში კი ეწვიეთ საიტს
- **https://haveibeenpwned.com/Passwords**. აქ თქვენ საშუალება გექნებათ შეამოწმოთ თქვენთვის სასურველი პაროლი ყოფილა თუ არა ოდესმე გატეხილ ანგარიშებს შორის დაფიქსირებული და თუ ყოფილა რამდენჯერ. მეტი დემონსტრაციისთვის შეგიძლიათ იხილოთ ვიდეო ქვევით, სადაც განხილულია ელექტრონული მეილების და პაროლების შემოწმება აღნიშნულ პლატფორმაზე.

Play Video

აღნიშნულ საიტზე შეგიძლიათ, დეტალურად ნახოთ რომელი პლატფორმებიდან იქნა თქვენი მონაცემები გაჟონილი.

ყველასათვის ცნობილია, რომ ტექნოლოგიები მუდმივად ვითარდება და რამდენადაც მზარდია ტექნოლოგიური სფერო, ასევე იზრდება კიბერთავდასხმის ტაქტიკები, ტექნიკები და პროცედურები. დღესდღეობით მარტივი პაროლის გატეხვა რამდენიმე წამის, შესაძლოა მილიწამის საქმეს წარმოადგენდეს. ამიტომაც, უსაფრთხოების სპეციალისტები მუშაობენ ისეთ ავტორიზაციის მექანიზმებზე, რომლის მანიპულირებაც ნაკლებად შესაძლებელია. ასეთ მექანიზმებს მიეკუთვნება ბიომეტრიული და თერმული სკანერები, ქცევის ანალიზის სენსორი, ასევე მოძრაობის მანერის ანალიზი და უამრავი სხვა, რაც ძირითადად განასხვავებს ადამიანებს ერთმანეთისაგან.

ბიომეტრიული სკანერები საშუალებას გვაძლევენ, ავტორიზაცია გავიაროთ ძირითადად სახის, თვალის ბადურის, თითის ან ხელის ანაბეჭდის და ხმის მეშვეობით. ვინაიდან ყველა ადამიანი განსხვავებულია, დამატებითი თავდაცვის სახით შეგვიძლია აქაც მივმართოთ ორმაგ ავთენტიფიკაციას და რამდენიმე ბიომეტრიული მექანიზმი გამოვიყენოთ, მაგალითად თვალის ბადურის ანალიზი და თითის ანაბეჭდი.

პაროლების განახლება

პაროლების განახლების შესახებ სხვადასხვა საერთაშორისო სტანდარტში სხვადასხვა მიდგომა არსებობს. NIST (National Institute of Standards and Technology) ამერიკული სტანდარტის მიეხდვით პაროლი წელიწადში ერთხელ უნდა განვაახლოთ. ISO 27001-ს მიხედვით, პაროლის გამოცვლა რეკომენდებულია ყოველ 90 დღეში. სხვა წყაროებში კი ვხვდებით ისეთ მიდგომებს, რომლებიც მაგალითად მეტად კომპლექსური პაროლის შექმნას (მაგ: 25+ სიმბოლოიანი) უჭერენ მხარს, ვიდრე კვარტალში ან წელიწადში ერთხელ პაროლის გამოცვლას.

საბოლოოდ რეკომენდაციის სახით გეტყვით რომ, ოპტიმალური მიდგომა პაროლის **3 თვეში ერთხელ** შეცვლაა ასევე ძლიერი და კომპლექსური პაროლით, რომელიც წინისგან განსხვავებული იქნება და უნიკალური

რა არის ელექტრონული ფოსტის უსაფრთხოება?

კიბერუსაფრთხოების ერთ-ერთ მნიშვნელოვან საკითხს წარმოადგენს ელ-ფოსტის უსაფრთხოება და აუცილებელია მომხმარებელმა იცოდეს მასთან დაკავშირებული რისკები. აღსანიშნავია, რომ ზოგადად ელ-ფოსტა საკმაოდ ძველი სერვისია, თუმცა დღემდე აქტიურად იყენებენ როგორც ორგანიზაციები, ასევე ინდივიდუალური პირები. სტატისტიკურად კიბერშეტევების უმეტესობა სწორედ ამ გზით ხორციელდება. ამდენად, მნიშვნელოვანია მისი რისკებისა და შესაბამისი დამცავი ზომების გაცნობიერება. კიბერდამნაშავეებს ფართო გზა ეძლევათ იმისთვის, რომ მეილ-სერვერისა და ელექტრონული წერილის მეშვეობით სხვადასხვა სახის კიბერშეტევების ვექტორები გამოიყენონ და ორგანიზაციების თანამშრომლებზე კიბერშეტევები განახორციელონ.

ელექტრონული ფოსტის უსაფრთხოების თავში განხილული იქნება ყველა ის შესაძლო საფრთხეები, რომელიც შეიძლება ელექტრონული ფოსტით მიადგეს როგორც ფიზიკურ პირს, ისე ნებისმიერ ორგანიზაციას. ესენია:

სპამი;

ფიშინგი;

საეჭვო ბმულები მეილში;

მავნე ფაილები;

კონფიდენციალური მონაცემების გაზიარება.

ელ-ფოსტა ძალიან პოპულარული საბაზისო ქსელური მომსახურებაა, რომელსაც გარკვეული უპირატესობა აქვს ინფორმაციის მიმოცვლის თვალსაზრისით. ერთის მხრივ, ელ-ფოსტით კომუნიკაცია ცვლის შრომით ჩვევებსა და ურთიერთობებს ორგანიზაციასა და თანამშრომლებს შორის, თუმცა, მეორეს მხრივ, არსებობს ბევრი რისკი, რადგან ამ მომსახურებას ბევრი პოტენციური სისუსტე გააჩნია, მაგალითად: არაავტორიზებული წვდომა მონაცემებზე, მონაცემების შეცვლა, მონაცემებისა და ფაილების უსაფრთხოების რისკი და ა.შ.

ელექტრონული წერილების გაგზავნის პროცესში ყურადღება უნდა მიექცეს მესიჯების კონფიდენციალურობასა და ავთენტურობას. ელ-ფოსტით მესიჯების გაგზავნა იგივეა, რაც ღია ბარათის გაგზავნა, მისი შინაარსი წაკითხვადია და აღნიშნული შინაარსის არასასურველი შეცვლისგან თავის ასარიდებლად საჭიროა შესაბამისი უსაფრთხოების ზომების მიღება.

ელექტრონული ფოსტით კომუნიკაცია ითვლება ღია და არც თუ ისე დაცულ საკომუნიკაციო მეთოდად, თუ თქვენ არ იყენებთ **PGP (Pretty Good Privacy)** მეთოდს (იხ. ვრცლად მე-8 თავში), რომელიც საშუალებას იძლევა, წერილები დაშიფროთ და მხოლოდ მიმღებმა გახსნას თავისი კუთვნილი მისამართით. დოკუმენტის დაშიფვრა შესაძლებელია პაროლის დადებით. მომხმარებელს შეუძლია ZIP ფაილის შექმნა, პაროლით დაცვა და ამის შემდეგ გაგზავნა, ან გამოიყენეთ მეილების შიფრაციით გაგზავნის მეთოდი, რომელსაც ეწოდება PGP.

ელექტრონული ფოსტა ასევე გამოიყენება სარეკლამო მეილების, ვირუსების, ფიშინგების და სხვა მავნე შინაარსის მეილების გასაგზავნად. ელექტრონული ფოსტის წყაროს ანუ გამგზავნის გაყალბება კიბერდამნაშავეებისთვის ძალიან მარტივია.

ელექტრონული ფოსტის აპლიკაციები (Outlook, Gmail, Yahoo, და ა.შ.)

მნიშვნელოვანია ელექტრონული ფოსტის აპლიკაციების სწორი გამოყენება, რაშიც იგულისხმება ის, რომ აპლიკაციები უნდა იყოს სანდო წყაროებიდან გადმოწერილი და სერთიფიცირებული კომპანიების მიერ შექმნილი.

სხვადასხვა გაურკვეველი წყაროებიდან გადმოწერილი აპლიკაცია შეიძლება შეიცავდეს მავნე ფაილს ან განთავსებული იყოს მასში სხვადასხვა ტიპის მავნე პროგრამა (ტროიანი, ბოტნეტი და ა.შ.), რომელიც თქვენს პირად ინფორმაციას იპარავს. სწორედ ამიტომ, არ უნდა გადმოწეროთ აპლიკაციები ტორენტებიდან (იხ. ვრცლად მე-5 თავი) და სხვა არასანდო ვებ-გვერდებიდან. ასევე აუცილებელია, რომ მუდმივად გაანახლოთ ის ელექტრონული ფოსტის აპლიკაცია, რომელსაც მოიხმართ სისტემატიურად, რადგან

ხშირად კიბერდამნაშავეები იყენებენ სხვადასხვა ტიპის სისუსტეებს აპლიკაციებზე, რომლებიც ძველ (მოწყვლად) ვერსიებზე მუშაობენ.

რა არის სპამი?

ყოველდღიურად სპამი ეგზავნებათ ბევრ მომხმარებელს რეკლამირების, ფიშინგის, ან მავნე ფაილების გავრცელების მიზნით. ელ-ფოსტა არ არის ინფორმაციის გაცვლის უსაფრთხო საშუალება და არ არის რთული უამრავი მეილის გაგზავნა ყალბი გამომგზავნის სახელით.

სპამი ეგზავნება ძალიან ბევრ მიმღებს, მაგრამ ალბათ გიჩნდებათ შეკითხვა: როგორ იგებენ კიბერდამნაშავეები ელ-ფოსტის მისამართებს? მათ სხვადასხვა წყაროები აქვთ. შესაძლოა შემტევმა შავ ბაზარზე გაყიდოს მისამართების სია, მაგალითად, 1 000 000 ლეგიტიმური მისამართი 170 აშშ დოლარად, ან მისამართებს იღებენ სოციალური ქსელებიდან, ფორუმებიდან და ა.შ. ამიტომ ფრთხილად იყავით, როდესაც თქვენი ელ-ფოსტის მისამართს უთითებთ ამგვარ სერვისებში.

სტატისტიკურად მთლიანი ელექტრონული წერილების ნაკადის დაახლოებით 85%-მდე სპამს წარმოადგენს. სპამ მეილების უმეტესობა მოდის აშშ-დან, რუსეთიდან, ინდოეთიდან და სხვა ქვეყნებიდან.

სპამ ფილტრს თქვენი მეილის კლიენტებზე შეუძლია სპამ მეილი ამოიცნოს. თუ გაქვთ სპამ მეილი, მონიშნეთ მეილ კლიენტში როგორც „სპამი" და ამის შემდეგ წაშალეთ.

როგორ დავბლოკოთ სპამ მეილების გამომგზავნი?

სპამ მეილებში წარმოდგენილი ბმულები არც ისე სანდოა, როგორც ერთი შეხედვით ჩანს. უმეტეს შემთხვევაში, მოცემული ბმულები აკავშირებს მომხმარებელს ინფიცირებულ ვებგვერდებთან ან აიძულებს ჩამოტვირთონ ვირუსები, რომლებიც მიზნად ისახავენ მოწყობილობის დაინფიცირებას და მონაცემთა მოპარვას.

სურათზე ხედავთ Gmail ანგარიშს სადაც განთავსებულია სხვადასხვა ელექტრონული წერილები, რომლებიც გახლავთ საფრთხის შემცველი. მოცემულ ბმულებზე, დიდი ალბათობით, არის ვირუსი ან ფიშინგი, რის შემდეგაც კიბერდამნაშავეები ან აინფიცირებენ კომპიუტერს, ან იპარავენ სხვადასხვა კონფიდენციალურ ინფორმაციას.

რა არის ფიშინგი?

ფიშინგი (ინგლისურად „phishing“) - ინტერნეტ თაღლითობის დანაშაულებრივი ფორმაა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები (მაგ.: პაროლი, საკრედიტო ბარათის ან საბანკო ანაგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია). Spear ფიშინგი არის ფიშინგის ერთ-ერთი სახეობა, როდესაც კიბერდამნაშავე მსხვერპლად ირჩევს ერთ კონკრეტულ პირს, ჯგუფს ან ორგანიზაციას. Whale ფიშინგი/Whaling-ის დროს კი თავდამსხმელი მიზანში იღებს ორგანიზაციების და მსხვილი კომპანიების ხელმძღვანელებსა და მფლობელებს.

ფიშინგისას შენიღბული ინტერნეტ კომუნიკაციის საშუალებით ხდება მომხმარებლის შესახებ ისეთი ინფორმაციის მოპოვება, როგორიცაა მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი. ეს მიიღწევა შემდეგი მეთოდებით: ელექტრონული წერილების მასობრივი დაგზავნით (წერილის ავტორებად იყენებენ ცნობილ ორგანიზაციებს და ბრენდებს), ასევე პირადი შეტყობინებებით (მეილ სერვერების გამოყენებითა და სოციალური ქსელების საშუალებებით), რომლებშიც გამოყენებულია ბანკის სახელი. წერილში ხშირად არის ვებგვერდის ბმული, რომლის ვიზუალური მხარე არ განსხვავდება ნამდვილისგან. შესაბამისად, გაყალბებულ ვებგვერდზე შეტანილი ინფორმაცია კიბერდამნაშავის ხელში ხვდება ავტომატურად. ხშირად, მათთვის, ვინც შეტევას ახორციელებს, ინგლისური და ქართული არ არის მშობლიური ენა, ამიტომ

წერილში ბევრი შეცდომაა, როდესაც ამგვარ რამეს შეამჩნევთ, გამოიჩინეთ მეტი სიფრთხილე. თუ თვლით რომ შემოსული შეტყობინება ლეგიტიმურია, გადაამოწმეთ ტელეფონით. დააკვირდით ასევე ბმულებს, ნამდვილად ეკუთვნის თუ არა ბმული გამომგზავნ ორგანიზაციას, ასევე გადაამოწმეთ აღნიშნულ ვებგვერდს თუ გააჩნია უსაფრთხოების სერთიფიკატი.

ფიშინგი შესაძლოა განხორციელდეს ინტერნეტის საშუალებით, მობილური ზარით ან თუნდაც მობილური შეტყობინებით. ინტერნეტ ფიშინგი არის, როდესაც კიბერდამნაშავე ინტერნეტის მეშვეობით ცდილობს თქვენი მონაცემების მოპარვას; როგორიცაა ვთქვათ რომელიმე პორტალის ან ელექტრონული ფოსტის მომხმარებლის სახელი ან პაროლი. მაგალითად, როდესაც კიბერდამნაშავე გამოგიგზავნით ელექტრონული ფოსტით შეტყობინებას, რომ მეილ სერვერზე მიმდინარეობს სამუშაოები და თქვენი ელექტრონული ანგარიში რომ არ წაიშალოს, აუცილებლად უნდა მიაწოდოთ თქვენი მომხმარებლის სახელი ან პაროლი. ასევე, როდესაც მოტყუებით შეგიყვანთ თქვენი ორგანიზაციის კუთვნილი ვებმეილის ანალოგიურ გვერდზე და იქ გაგატარებთ ავტორიზაციას.

მობილური ზარით ფიშინგი - „ვიშინგი“ ხორციელდება ტელეფონით, როდესაც მოტყუებით გირეკავენ იმ კომპანიის სახელით, რომლის კლიენტიც თქვენ ბრძანდებით და ცდილობენ თქვენი ინფორმაციის მოპარვას. ზუსტად ანალოგიურია მობილური შეტყობინებით ფიშინგი - „სმიშინგი“, ინფორმაციის მოპარვა ხორციელდება სმს მეთოდის გამოყენებით.

სურათზე თქვენ ხედავთ მაგალითს, სადაც ნაჩვენებია ელექტრონული წერილის ფიშინგის ნიმუში. ეს არის შეტყობინება ვითომ ამაზონიდან, მაგრამ თუ დააკვირდებით დეტალებს, ბევრ უზუსტობას აღმოაჩენთ. პირველ რიგში, აუცილებელია, შეხედოთ თუ საიდან მიიღეთ წერილი: წერილი გამოგზავნილია არა „amazon.com“ დომეინიდან, არამედ „mazoncanada.ca“ დომეინიდან, რაც უკვე იმის მანიშნებელია რომ წერილი კომპანია ამაზონიდან არ არის გამოგზავნილი.

ასევე, სანდო და რეპუტაციული კომპანიები, როგორსაც მიეკუთვნება ამაზონი, თავიანთ კლიენტებს მიმართავენ ყოველთვის სახელით, რადგან მათ გააჩნიათ თავიანთი მომხმარებლების მონაცემთა ბაზა. რაც შეეხება კიბერდამნაშავეებს, მათ შეიძლება არ იცოდნენ კონკრეტული სახელი და წერილი იყოს. ზოგადად დაწერილი, როგორც კლიენტი. ამ შემთხვევაში შეიძლება დაეჭვდეთ და ამგვარ მეილებთან უფრო მეტი სიფრთხილე გამოიჩინოთ.

და ბოლოს, აუცილებელია ყველა საეჭვო მეილში, სადაც განთავსებულია ბმულები, მაუსის კურსორი მიიტანოთ და გამოჩენილ ფანჯარაში ან ვებბრაუზერის ქვედა მარცხენა კუთხეში წაიკითხოთ, თუ სად ხდება გადამისამართება. სურათზე ვიზუალურად დაინახავთ, რომ ამაზონის ვებ გვერდის მაგივრად, კიბერდამნაშავე მოტყუებით ცდილობს, რომ მომხმარებელი შეიყვანოს „kereskedj.com“ მისამართზე, სადაც თქვენ ან მავნე ფაილის გადმოწერას დაიწყებთ ან მოხვდებით ამაზონის ანალოგიურ, ფიშინგ ავტორიზაციის ვებ გვერდზე, სადაც მოგთხოვენ სახელსა და პაროლს, რომლის შეყვანის შემთხვევაში კიბერდამნაშავეები თქვენს მონაცემებზე წვდომას მოიპოვებენ.

საეჭვო ბმულები მეილში

გარკვეულ შემთხვევებში, კიბერდამნაშავეს სჭირდება, რომ თქვენ მხოლოდ დააწკაპუნოთ ბმულზე და თქვენი ბრაუზერით გახსნათ მავნე ფაილის შემცველი გვერდი. ამ შემთხვევაში თქვენი ორგანიზაცია რისკის ქვეშაა. მაშინაც კი თუ ბმული ერთი შეხედვით ნორმალურად გამოიყურება, უნდა დარწმუნდეთ, რომ ის რეალურია. ამ სიტუაციაში გადაწყვეტილების მისაღებად საჭიროა დაფიქრება და ბმულის დეტალურად გადამოწმება. ამის შესამოწმებლად საჭიროა, მიიტანოთ მაუსის კურსორი ბმულთან, მასზე დაკლიკების გარეშე. ქვედა მარცხენა კუთხეში დაინახავთ ბმულის უკან არსებულ, რეალურ მისამართს. დარწმუნდით, რომ რეალური მისამართი სანდოა და მხოლოდ ამის შემდგომ გახსენით.

ასევე საყურადღებოა შემოკლებული ბმულები, რომლებიც უმეტეს შემთხვევაში ბოროტულ მიზანს ემსახურება. ამის თავიდან ასარიდებლად კი მხოლოდ ბმულის სანდოობაში დარწმუნებაა საჭირო.

მავნე ფაილები

ჩვეულებრივი მომხმარებელი ხშირად ელექტრონულ წერილს ბოლომდე არ კითხულობს და თანდართულ ფაილზე აწკაპუნებს, განსაკუთრებით როდესაც საფოსტო ბარათებს გზავნიან (დღესასწაულებზე და შეხვედრებზე).

ხშირად ვირუსი დაარქივებული ZIP ფაილის სახით მოდის, როდესაც დაცულია პაროლით და ანტივირუსი ვერ ახერხებს ამგვარი ფაილის ავტომატურად დაბლოკვას. ამ შემთხვევაში, საჭიროა ორგანიზაციასთან გადაამოწმოთ პაროლის საჭიროება და გამოგზავნილი ფაილის უსაფრთხოება. მავნე ფაილების გავრცელება აინფიცირებს თქვენი ორგანიზაციის კომპიუტერს. როდესაც ვირუსი შედის კომპიუტერში, ტექნიკური ჯგუფი მის კონტროლს ვეღარ ახერხებს.

ეს რაც პირველ ფაზაზე ხდება, სხვა ფაზები დამოკიდებულია შეტევის მიზანზე ან მოტივაციაზე; ხანდახან თქვენ რესურსებს ან ინფრასტრუქტურას სხვა ორგანიზაციაზე შეტევისთვის იყენებენ. ერთ-ერთი გზაა თუ დაშიფრავენ თქვენს ინფორმაციას და მის განსაშიფრად მოგთხოვენ გამოსასყიდს.

ინფორმაციის მოპარვა ხშირად არის მოტივაცია შეტევისთვის და ამისთვის ერთ-ერთი მეთოდი არის ფიშინგის მეილის გაგზავნა ინფიცირებული ფაილით. სურათზე თქვენ ხედავთ მაგალითს, სადაც კიბერდამნაშავე აგზავნის CV-ის. ერთი შეხედვით ჩანს, რომ ეს არის ლეგიტიმური წერილი, მაგრამ ასევე აგზავნის პაროლს. სავარაუდოდ, მოცემული ფაილი არა ვორდის ფაილი, არამედ რაიმე პროგრამაა, რომელიც შეიძლება იყოს დაარქივებული სახით.

ხშირად, კიბერდამნაშავეები აარქივებენ თავიანთ ვირუსებს და ადებენ პაროლს, რომ ამით თავი აარიდონ ანტივირუსებს. ასევე იყენებენ გაშვებად მიმაგრებულ ფაილებს (*.vbs, *.pif, *.exe) უცნაური სახელებით, მაგალითად, როგორიცაა: „invoice-290348.zip“.

საეჭვო ან მავნე მიმაგრებული ფაილი ჩვეულებრივ მოდის უცნობი პირისგან. შეტყობინების საგნის ადგილას ხშირად წერია ერთჯერადი შეთავაზება ან მოწოდება მოქმედებისთვის ან რაღაც ისეთი, რაც უბიძგებს მიმღებს დაუყოვნებლივ გახსნას მიმაგრებული ფაილი.

კიბერთავდასხმისგან თავის ასარიდებლად, აუცილებელი პირობაა რთული პაროლის შემუშავება. მარტივი პაროლის შემთხვევაში თავდამსხმელს საქმეს ძალიან გავუმარტივებთ. არ დააყენოთ ხშირად გამოყენებადი პაროლები (12345678, password123 და ა.შ.). ეცადეთ პაროლი იყოს მრავალფეროვანი, შეიცავდეს დიდ და პატარა ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს (@, !, $) და შეეცადეთ პერიოდულად გამოცვალოთ (იხ. ვრცლად მე-3 თავი).

როგორ უზრუნველყოთ ელექტრონული ფოსტის უსაფრთხოება?

არასოდეს გახსნათ უცნობი პირისგან გამოგზავნილი ელექტრონულ წერილი.

არასოდეს გახსნათ ნაცნობი პირისგან გამოგზავნილ ელექტრონულ წერილში უცნაური დასახელების მიმაგრებული ფაილები.

ყოველთვის ყურადღებით იყავით უცნობი წყაროსაგან მიღებულ წერილთან, ზედმეტად სარგებლის მომტანი შინაარსის მქონე შეტყობინებებთან.

არასოდეს გახსნათ მიმაგრებული ფაილი, თუ დარწმუნებული არ ხართ მათ სანდოობაში.

მუდმივად განაახლეთ ანტივირუსი და ხშირად მოხმარებადი პროგრამები.

ფრთხილად იყავით მაკროსის (Macros) შემცველ და პაროლით დაცულ დოკუმენტებთან.

გამოიყენეთ კომპლექსური პაროლები.

ნებისმიერ საეჭვო ვითარებაში დაუკავშირდით ტექნიკური დახმარების ჯგუფს.

აქტივობის შემოწმება ელ-ფოსტის ანგარიშზე

ასევე მნიშვნელოვანია თუ თქვენს მეილ სერვერს გააჩნია აქტივობების შემოწმების ფუნქცია, პერიოდულად ან რაიმე გაუგებარი სიტუაციის დროს შეამოწმოთ თქვენი ელ. ფოსტის ანგარიშის აქტივობები. მაგალითად, თუ თქვენ სარგებლობთ Gmail-ის სერვისით, მთავარ პანელში, მარჯვენა ქვედა კუთხეში შეგიძლიათ ნახოთ „Last account activity“ ბმული, სადაც გადასვლის შემდეგ თქვენ დაინახავთ აქტივობებს თუ ვის მიერ ხდებოდა თქვენი მეილის ანგარიშზე წვდომა.

მაგალითად, თუ შეხედავთ სურათს, პირველ განყოფილებაში შეგიძლიათ ნახოთ თუ რა ტიპის წვდომა განხორციელდა თქვენს ელექტრონული ფოსტის ანგარიშზე. სურათზე ჩანს, რომ წვდომა განხორციელდა ვებბრაუზერიდან, მობილურიდან და IMAP-დან (IMAP

ნიშნავს, რომ წვდომა განხორციელდა რომელიმე მეილის
აპლიკაციიდან, მაგალითად Outlook-დან).

მეორე განყოფილებაში, რომელიც გახლავთ ლოკაციისა და IP მისამართების განყოფილება, თქვენ შეგიძლიათ დაადგინოთ თუ რომელი ქვეყნიდან განხორციელდა წვდომა თქვენი ელექტრონული ფოსტის ანგარიშზე ან დაადგინოთ კონკრეტული IP მისამართი, რის მიხედვითაც შესაძლებელია იმის დასტური, რომ ნამდვილად თქვენ შეხვედით კონკრეტულ ანგარიშზე.

მესამე განყოფილებაში თქვენ შეგიძლიათ შეამოწმოთ ელექტრონული ფოსტის ანგარიშზე შესვლის თარიღები და დროები. აღნიშნული ინფორმაცია საშუალებას გაძლევთ, აწარმოოთ საკუთარი ელ-ფოსტის მონიტორინგი და უცხო პირის მიერ მისი გამოყენების შემთხვევაში მიიღოთ დაუყოვნებლივი ზომები.

AD BLOCKER

ინტერნეტში არსებული საიტების უმრავლესობა არის უფასო. ლოგიკურია რომ ამ საიტების ავტორებს სურთ რაიმე გზით ფინანსური მოგებაც ნახონ თავიანთი შრომიდან. ყველაზე მარტივი გზა ამის მისაღწევად არის საიტზე რეკლამების განთავსება. საიტზე რეკლამები გვხვდება მთავარი ტექსტის გვერდებზე, დასაწყისში და დასასრულს. ხშირია ასევე ტექსტის შუაში რეკლამებიც. ხშირად ვებგვერდის ავტორებს არ გააჩნიათ დიდი კონტროლი იმაზე თუ რომელი რეკლამები განთავსდება მათ საიტზე. ისინი ამჯობინებენ რეკლამების შერჩევა და ცვლა მოხდეს ავტომატურად და მათ მხოლოდ ფინანსური სარგებელი მიიღონ. ამის გამო, ვებგვერდებზე რეკლამების განთავსება შეუძლიათ ბოროტმოქმედებსაც. ასეთი რეკლამები, მკვეთრი ფერებით და ყურადღების მიმქცევი მესიჯებით ცდილობენ მომხმარებლის ყურადღების მიქცევას.

რეკლამაზე დაჭერის შემდეგ შეიძლება ავტომატურად გაიხსნას ისეთი საიტი, რომელიც ინფორმაციის მოპარვას ცდილობს. ასევე არის შანსი, რომ ავტომატურად გადმოიწეროს რაიმე ფაილი, რომელიც არცერთ შემთხვევაში არ უნდა გაეშვას და უმჯობესია წაიშალოს.

პირველ რიგში, ნებისმიერ ბრაუზერში უნდა იყოს დაყენებული “uBlock Origin”. იგი ავტომატურად ბევრი ისეთი საფრთხისაგან დაგიცავთ, როგორიცაა მაგალითად ე.წ. “pop-up” რეკლამები, რომლის დროსაც ვლინდება ბევრი თაღლითური საიტები და ფიშინგი. ერთ-ერთი ყველაზე ცნობილი თაღლითობის ტიპია „თქვენს კომპიუტერს აქვს ვირუსი“; ან შეტყობინებები, რომლებიც პირდაპირ ითხოვენ ფულის გადარიცხვას, რადგან თითქოს თქვენ დაარღვიეთ კანონი და უნდა გადაიხადოთ ჯარიმა სახელმწიფოს ანგარიშზე, წინააღმდეგ შემთხვევაში დაიწყება სისხლის სამართლის დევნა თქვენს წინააღმდეგ.

მოცემულ ფოტოზე ნაჩვენებია მსგავსი Pop-Up რეკლამა, სადაც მოცემულ ბმულებზე გადასვლისას იხსნება ვებგვერდი, რომელიც შესაძლოა შეიცავდეს სხვადასხვა ტიპის საფრთხეს, მაგალითად: Trojan, Virus, Ransomware, Malware. როგორც უკვე აღინიშნა, მსგავსი რისკების თავიდან აცილება შესაძლებელია uBlock Origin-ის საშუალებით, თუმცა არსებობს საიტები, რომლებიც ითხოვენ ad blocker-ების გათიშვას, რათა გამოიყენოთ მათი სერვისები, ამიტომ აუცილებელია იცოდეთ, თუ როგორ უნდა მოიქცეთ ასეთ შემთხვევაში. Virustotal არის ხელსაწყო-პლატფორმა, სადაც შეგიძლიათ, გადაამოწმოთ არა მხოლოდ ფაილები და აპლიკაციები, არამედ ბმულებიც. გაითვალისწინეთ, რომ ყოველთვის 100%-ით სანდო შედეგები შეიძლება არ იყოს და შესაბამისად საჭიროა საბაზისო ცოდნა და სიფრთხილე ნებისმიერი ბმულისა და ფაილის გადმოწერისას.

Play Video

შემდეგი ნაბიჯია ე.წ. “Cookie”-ის შემოწმება. Cookie არის პატარა ტექსტის ნაწყვეტები, რომელიც იგზავნება თქვენს ბრაუზერთან იმ საიტის მიერ, რომელზეც შედიხართ. ისინი იმახსოვრებენ სხვადასხვა ინფორმაციას ვებგვერდის გამოყენებისას, რაც სამომავლოდ აადვილებს საიტის განმეორებით გამოყენებას, მაგრამ Cookie-ებით ასევე შეიძლება სხვადასხვა პირადი ინფორმაციის დამახსოვრებაც, რომლის მეშვეობითაც უკვე შესაძლოა თქვენს მიმართ გამოყენებული იქნას ე.წ. მიზანმიმართული რეკლამები (Targeted Ads). ყველაზე გავრცელებული პრაქტიკაა, როდესაც გუგლში მოიძიეთ რაიმე პროდუქტი და მომდევნო კვირის განმავლობაში გხვდებათ მხოლოდ ამ პროდუქტთან დაკავშირებული რეკლამები. ამიტომ აუცილებელია საიტის გამოყენებისას Cookie პოლიტიკაში მიუთითოთ მხოლოდ ის ველები, რომლებიც გსურთ და გამორთოთ სხვა თქვენთვის არასასურველი ვარიანტები.

წარმოდგენილ სურათში ჩანს ნაკლებად აგრესიული ტიპის Cookie-ები:

ხოლო ამ ვარიანტში მოცემულია უფრო აგრესიული ფორმა, სადაც წარმოდგენილია სამი ვარიანტი: თანხმობა ყველაფერზე, მხოლოდ საჭიროზე ან შუაში თეთრი ღილაკით სასურველი ვარიანტების ხელით არჩევა.

აუცილებლად უნდა დაუკვირდეთ ღილაკებსაც. ზოგადად თანხმობის ღილაკები გაფერადებულია ყურადღების მისაქცევად, ხოლო უარყოფის ღილაკები ფაქტობრივად შეუმჩნეველია.

HTTP VS HTTPS

ინტერნეტის გამოყენებისას საიტებსა და მომხმარებლებს შორის ინფორმაციის მიმოცვლა ხდება HTTP პროტოკოლის გამოყენებით. HyperText Transfer Protocol - http ზოგადად ნიშნავს,

რომ საიტს არ გააჩნია SSL ან TLS სერტიფიკატი და საიტი დაუცველია. თავდაპირველ იმპლემენტაციაში http იყო დაუშიფრავი, რაც ნიშნავს იმას, რომ ქსელური ინფრასტრუქტურის მფლობელს შეეძლო მომხმარებელსა და ვებგვერდის სერვერს შორის ინფორმაციის წაკითხვა და ზოგიერთ შემთხვევაში მავნე მიზნებით ჩასწორებაც კი. ამ საფრთხის აღმოსაფრხველად შეიქმნა https. S=Secure, ანუ დაცული. https-ს გამოყენებისას ინფორმაცია კომპიუტერსა და სერვერს შორის არის დაშიფრული და მისი წაკითხვა არავის შეუძლია ქსელის რომელიმე ნაწილზე მოსმენის გზით.

სამწუხაროდ საიტების ზოგიერთი ნაწილი ჯერ კიდევ არ იყენებს https-ს და მხოლოდ http-ს მეშვეობით იცვლება ინფორმაცია. ამ საიტებზე შესვლისას ბრაუზერი ატყობინებს მომხმარებელს დაუცველი კომუნიკციის შესახებ. ამის გადასამოწმებლად უნდა დააკვირდეთ ზედა მარცხენა კუთხეში არსებულ ბოქლომის სიმბოლოს. თუ ეს ბოქლომის სიმბოლო არ არის გაწითლებული ან გადახაზული, შესაბამისად დამყარებული კომუნიკაცია დაცულია.

დაუცველია:

ისეთ საიტებზე, რომლებიც არ იყენებენ https პროტოკოლს, არ შეიყვანოთ ისეთი პირადი ინფორმაცია, როგორიცაა ელ. ფოსტა, პაროლი, მისამართი, ტელეფონის ნომერი, ბარათის მონაცემები და ა.შ., რადგან არსებობს მათი მოპარვის საფრთხე. HTTPS აბათილებს პოტენციურ person-in-the-middle შეტევებს. ისეთი სერვისები, როგორებიცაა ელექტრონული ყიდვა-გაყიდვა და ბანკები, იყენებენ მხოლოდ HTTPS ვებგვერდებს. აუცილებელია, დაუკვირდეთ დაცულია თუ არა ვებგვერდი სანამ მის გამოყენებას დაიწყებთ.

VPN

როგორც უკვე აღინიშნა, ვებსაიტების დიდი ნაწილი იყენებს https პროტოკოლს, თუმცა ინფორმაციის ნაწილი მაინც დაუშიფრავად იგზავნება ქსელში. ამის ყველაზე ცალსახა მაგალითი არის DNS (Domain Name System). მისი მეშვეობით ხდება ვებგვერდის სახელების გადაყვანა IP მისამართებში. ვებგვერდის გახსნისას მომხმარებლის მოწყობილობიდან იგზავნება კითხვა, რომელიც ვებგვერდის დომენს შეიცავს. ეს კითხვა ქსელში მოგზაურობისას სრულიად დაუშიფრავია და გზაზე ნებისმიერ პირს შეუძლია დაინახოს თუ რომელ საიტზე ცდილობთ შესვლას. უნდა აღინიშნოს ისიც, რომ ისინი სახელთან ერთად ვერ ხედავენ კონკრეტულ გვერდს, რომელზეც შესული ხართ. მაგალითად, არ შეუძლიათ გაიგონ თუ რომელ ვიდეოს უყურებთ youtube-ზე. ამ ინფორმაციის ზოგიერთი პირებისაგან დამალვის ერთ-ერთი მეთოდი არის VPN-ის გამოყენება.

VPN (Virtual Private Networks) ქმნის დაცულ და დაშიფრულ ბმას მომხმარებლის მოწყობილობიდან სხვა სერვერთან დასაკავშირებლად, რომლის გამოყენებითაც იხსნება დაშიფრული "გვირაბი" მომხდმარებელსა და სერვერს შორის (რომელიც უმეტესად სხვა ქვეყანაშია). მომხმარებლის მიერ გაგზავნილი ყველა მოთხოვნა ჯერ ამ გვირაბში გადის და შემდეგ VPN სერვერის სახელით იგზავნება სამიზნემდე. იგი ნიღბავს მომხმარებლის IP მისამართს და შიფრავს ინფორმაციის მიმოცვლას. VPN-ის გამოყენებით შენიღბული IP მისამართი ურთულებს ვებგვერდებს და სერვისებს თქვენი აქტივობის მეთვალყურეობას ციფრულ სივრცეში. მისი მეშვეობით შესაძლებელია პირადი მონაცემების დაცვა და მიზანმიმართული რეკლამების შემცირება. VPN ასევე წარმოადგენს დამატებითი უსაფრთხოების ფენასაც ელექტროკომუნიკაციისას. ეს განსაკუთრებით მნიშვნელოვანია, როდესაც იყენებთ საჯარო Wi-Fi ქსელს, სადაც ინფორმაციის მოპარვის რისკი უფრო მაღალია, მაგალითად, კაფეში ან აეროპორტში, რადგან ხშირად საჯარო უკაბელო ქსელი ნაკლებად დაცულია. VPN-ის გამოყენებით ინფორმაცია, შემტევმა რომც მოიპაროს, მისი წაკითხვა ბევრად რთული იქნება შიფრის გამო. VPN ასევე ართულებს ISP-ის (ინტერნეტ სერვის პროვაიდერი) მონიტორინგს და მომხმარებლის ინტერნეტის აქტივობის გაანალიზებას. VPN საჭიროა მათთვის, ვისთვისაც მნიშვნელოვანია პირადი მონაცემების დაცულობა და არ უნდათ, რომ მათზე შეგროვებული ინფორმაცია პოტენციურად გაყიდოს ISP-მ. VPN ასევე კარგია იმ ინდივიდებისათვის, ვინც მუშაობენ დისტანციურად ან უკავშირდებიან კორპორატიულ ქსელს.

ინკოგნიტო რეჟიმი

ბრაუზერში ჩაშენებული ინკოგნიტო რეჟიმი საშუალებას იძლევა, შედარებით უსაფრთხოდ გამოიყენოთ ინტერნეტი. მაგრამ, როგორც ყველაფერს, მასაც აქვს თავისი ლიმიტები და აუცილებელია მათი გათვალისწინება. ინკოგნიტოს რეჟიმი არ ინახავს ლოკალურად (ანუ ფიზიკურად თქვენს ბრაუზერში) თქვენს ვებისტორიას, საძიებო ველის ისტორიებს და Cookie-ებს. ეს ყველაზე გამოსადეგია ისეთ სიტუაციაში, როდესაც არ გსურთ, რომ ვინმემ ამოიღოს თქვენი კომპიუტერიდან თქვენი ბრაუზინგის ისტორია; ან თუ ხართ საზიარო კომპიუტერთან და არ გინდათ სხვა მომხმარებელმა ნახოს ის. თქვენს აქტივობას ასევე ხედავენ თქვენი ISP (ინტერნეტ სერვის პროვაიდერი), ქსელური ადმინისტრატორი და საიტები, რომლებსაც სტუმრობთ. ინკოგნიტო რეჟიმი ხელს არ უშლის საიტების ავტორების მიერ ინფორმაციის შეგროვებას და მიზანმიმართული რეკლამების გამოყენებას.

Torrents

ტორენტი არის დეცენტრალიზებული ფაილების გაზიარების მეთოდი, რომელიც განსხვავდება ტრადიციული ფაილების გაზიარების მეთოდისაგან, რასაც ჭირდება ცენტრალური სერვერი, სადაც განთავსებულია ეს ფაილები. ტორენტები აზიარებენ ფაილებს უშუალოდ მომხმარებლებს შორის. იგი არის პატარა ზომის ფაილი, რომელიც შეიცავს მეტადატას, ხოლო ტორენტის ტრეკერი არის სერვერი რომელიც ამყარებს კომუნიკაციას მომხმარებლებს შორის. Bittorrent არის პროტოკოლი, რომელიც ანაწევრებს ფაილებს და საშუალებას აძლევს მომხმარებლებს, გადმოტვირთონ ან ატვირთონ დანაწევრებული ფაილები ერთმანეთისაგან დამოუკიდებლად. ეს ნიშნავს უფრო სწრაფად და ეფექტურად ფაილების გაზიარებას. თვითონ ტორენტი ნეიტრალური ტექნოლოგიაა, მაგრამ შესაძლოა მისი არალეგალური და მავნე ფაილების გასაზიარებლად გამოყენება. ამიტომ უნდა უფრთხილდეთ და დაემორჩილოთ ადგილობრივ კანონმდებლობას, როდესაც იყენებთ ამ ტექნოლოგიას. ასევე აუცილებელია უფრთხილდეთ ცრუ ტორენტებს, რომლებიც შენიღბულია რაიმე რეალურ ფაილად და სინამდვილეში არის მავნე პროგრამული უზრუნველყოფა. ასევე ISP-ის (ინტერნეტ სერვის პროვაიდერს) შეუძლია თქვენი ტორენტების აქტივობის მონიტორინგი. ასევე არსებობს ორი სხვადასხვა მომხმარებლის ტიპი - Seeders და Leechers. Seeder-ები არიან მომხმარებლები, ვინც ჩაიწერეს მთლიანი ფაილი და დაიწყეს მისი გაზიარება სხვა მომხმარებლებთან. ეს ძალიან ეხმარება ტორენტის სიჯანსაღეს. თუ აღარ დარჩებიან Seeder მომხმარებლები და აღარავინ გააზიარებს ამ ფაილს, ტორენტი კვდება და მისი გამოყენება ფაქტობრივად შეუძლებელი ხდება. Leecher-ები არიან მომხმარებლები, ვინც თიშავენ გაზიარების ფუნქციას ან ჩართულნი არიან გადმოწერის პროცესში, მაგრამ ჯერ არ გადმოუწერიათ ფაილი სრულიად (ანუ ისინი ვერ გააზიარებენ მთლიან ფაილს).

ბრაუზერის ნებართვები

ზოგადად ვებგვერდებს ნორმალური ფუნქციონირებისას შეზღუდული აქვთ წვდომა მომხმარებლის კომპიუტერების რესურსების უმრავლესობაზე. მათ არ შეუძლიათ ფაილების წაკითხვა, ჩაწერა ნებისმიერ ადგილას, წვდომა კლავიატურაზე, კამერაზე ან მიკროფონზე. ამის მიუხედავად, მათ შეუძლიათ ჩამოთვლილთაგან ზოგიერთზე მოითხოვონ ნებართვა. ამის მარტივი მაგალითია ელექტრონული საკონფერენციო აპლიკაციები, როგორებიცაა, Zoom ან Google Meet. მათ ფუნქციონირებისათვის სჭირდებათ წვდომა მომხმარებლის კომპიუტერის მიკროფონსა და კამერაზე. როგორც წესი, წვდომაზე ნებართვის მიცემა ხდება

ვებგვერდის პირველი გამოყენების დროს. შემდეგ კი იგი იმახსოვრებს და ავტომატურად ჩართულია ან გამორთულია მომხმარებლის ნების შესაბამისად.

მნიშვნელოვანია რომ მსგავს ფანჯრებში წვდომის მიცემამდე კარგად დააკვირდეთ, თუ რომელი ვებგვერდია გახსნილი და რა ტიპის წვდომას ითხოვს იგი. წინააღმდეგ შემთხვევაში, შეიძლება ზოგიერთმა საიტმა დაუკითხავად ჩაიწეროს თქვენი საუბარი, გადაიღოს სურათი ან ვიდეო. განსაკუთრებით გავრცელებულია წვდომის მოთხოვნა შეტყობინების გაგზავნაზე. ამით ვებგვერდს შეუძლია გამოგზავნოს შეტყობინებები ბრაუზერის გარეთ. ეს შეტყობინება შეიძლება შეიცავდეს მავნე ლინკს, რომელზე გადასვლაც ზრდის მოწყობილობის დაინფიცირების რისკებს.

დღეს უამრავი სოციალური მედიის პლატფორმა გახდა როგორც პირადი, ისე პროფესიული ცხოვრების განუყოფელი ნაწილი. კომუნიკაციისა და ინფორმაციის გაზიარების შეუდარებელ შესაძლებლობებთან ერთად, აღნიშნული პლატფორმების გამოყენებასა და ინფორმაციის მიმოცვლას უამრავი საფრთხე ახლავს თან. შესაბამისად, ამ რისკების გაანალიზება და რეკომენდაციების გათვალისწინება აუცილებელია ჩვენი ციფრული უსაფრთხოებისათვის, განსაკუთრებით კი სენსიტიური ინფორმაციის დაცვისთვის.

სოციალურ მედიაში არსებული კიბერსაფრთხეები

აღნიშნულ ქვეთავში ვისაუბრებთ სოციალური მედიის პლატფორმებზე არსებულ კიბერსაფრთხეებსა და რისკებზე, რომლებიც ციფრული სამყაროს თანმდევი ნაწილია. ცნობიერების ამაღლება ამ საფრთხეების მრავალფეროვანი ბუნების შესახებ მნიშვნელოვან როლს ასრულებს მათ წინააღმდეგ ეფექტიანად ბრძოლაში.

სოციალურ ქსელებში ყველაზე გავრცელებულ საფრთხედ ფიშინგი მოიაზრება, რაც გულისხმობს მომხმარებლებისგან, მოტყუებით, პერსონალური ინფორმაციის მოპარვას (მათ შორის ელ. ფოსტის, პაროლის, საკრედიტო ბარათის მონაცემების და ა.შ.).

ამ მეთოდის გამოყენებით ბოროტმოქმედი ცდილობს, მომხმარებელი გადაიყვანოს ყალბ საიტზე და უბიძგოს მას პერსონალური ინფორმაციის გაზიარებისკენ. ეს უმეტესად ხდება გავრცელებული საიტების იდენტური საიტის აწყობით და მომხმარებლისათვის

ელექტრონული მეილის და პაროლის შეყვანის მოთხოვნით. ასეთი საიტების ამოსაცნობი მრავალი მეთოდი არსებობს. მაგალითად facebook.com-ის phishing საიტს შეიძლება ერქვას yourfacebook-sdfsdf.com ან რაიმე სხვა. ასევე უნდა შემოწმდეს მისი ფუნქციონალი, რამდენადაც ხშირად ასეთ საიტებზე ღილაკების დიდი ნაწილი არ მუშაობს. მე-5 თავში ნახსენები პლატფორმა virustotal.com დაგეხმარებათ, გადაამოწმოთ არის თუ არა ის უკვე დაფიქსირებული მავნე საიტების სიაში.

ფიშინგის გამოყენებით მოპარული მომხმარებლის სახელითა და პაროლით თავდამსხმელებს შეუძლიათ თქვენი სოციალური მედიის ანგარიშზე წვდომის მოპოვება და, შესაბამისად, საკმაო ზიანის მოყენება. აქედან გამომდინარე, იმისათვის, რომ თავდამსხმელებმა თქვენს ანგარიშებზე მომხმარებლის სახელითა და პაროლით შესვლა ვერ შეძლონ, აუცილებელია ორმაგი ავთენტიფიკაციის (2FA) გააქტიურება სოციალური მედიის ანგარიშებზე (დეტალური ინფორმაცია იხილეთ მე-3 თავში).

ამასთან, თავი შეიკავეთ სოციალური ქსელიდან ნებისმიერი სახის ფაილის გადმოწერისგან, ვინაიდან შესაძლებელია, აღნიშნული ფაილი მავნე ხასიათის იყოს. იქიდან გამომდინარე, რომ სოციალური მედია ინფორმაციის მიმოცვლის ერთ-ერთი ყველაზე სწრაფი და ეფექტური საშუალებაა, შესაბამისად, მარტივდება მავნე მოქმედებების განხორციელებაც.

გარდა ამისა, ხელოვნური ინტელექტის (Artificial Intelligence, შემდგომში AI) განვითარებასთან ერთად, მნიშვნელოვნად დაიხვეწა თავდამსხმელების შეტევის ტექნიკებიც. ე.წ. „DeepFake“ (არაავთენტური ვიდეოს გამოყენება რეპუტაციული ზიანის მიყენების მიზნით): დეზინფორმაციის მარტივად შექმნა და გავრცელება, დახვეწილი ფიშინგ წერილები – ეს ხელოვნური ინტელექტის ნაკლოვანებათა არასრული ჩამონათვალია. რამდენადაც რეგულაციებიც კი არ არსებობს მის წინააღმდეგ, თავდამსხმელებს საკმაოდ მარტივად შეუძლიათ ე.წ. AI-ს გამოყენება მავნე მიზნებისათვის. აღნიშნული პრობლემა არამარტო საქართველოში, არამედ მთელს მსოფლიოში დგას, ვინაიდან, იმ საფრთხეებისა და რისკების გაანალიზება, რაც ხელოვნურ ინტელექტს თან ახლავს, საკმაოდ დიდ რესურსთან და ძალისხმევასთან არის დაკავშირებული.

Play Video

ყურადსაღებია ასევე ე.წ. Third-Party - იგივე „მესამე მხარის“ აპლიკაციების გამოყენება სოციალური მედიის ანგარიშებით, რაც იმას ნიშნავს, რომ არ უნდა გამოიყენოთ სხვადასხვა ინტერნეტ-პლატფორმის ანგარიშები სხვა კონკრეტულ აპლიკაციასა თუ პლატფორმაზე ავტორიზაციისთვის. ყოველივე აქედან გამომდინარე, თუ რომელიმე ერთი მათგანი მაინც გახდა კიბერშეტევის სამიზნე, დიდი შანსია, რომ სხვა პირადი ინფორმაციაც აღმოჩნდეს თავდამსხმელების ხელში.

პირადი ინფორმაციის გაზიარების კონტროლი

როგორც უკვე აღინიშნა, დღევანდელ ეპოქაში, სადაც ციფრული სამყარო დომინირებს, ჩვენი პირადი ინფორმაციის დაცვა ერთ-ერთი მნიშვნელოვანი ფაქტორია უსაფრთხოების კუთხით. არსებობს სხვადასხვა ტიპის პირადი ინფორმაცია: თქვენი სრული სახელი, დაბადების თარიღი, მისამართი, ტელეფონის ნომერი, ფინანსური მონაცემები და ა.შ.

სოციალურ ქსელებში მათი გაზიარება შესაძლოა დასრულდეს საკმაოდ სავალალო შედეგებით - როგორც მატერიალური, ისე მორალური ზიანით.

თაღლითობა, შეიძლება ითქვას, რომ ინტერნეტ სივრცეში, განსაკუთრებით კი სოციალურ მედიაში, ერთ-ერთ დიდ საფრთხეს წარმოადგენს მომხმარებლებისათვის. თუ მომხმარებელი მუდმივად არ არის ყურადღებით, მსგავსი შეტევები თავდამსხმელების მხრიდან საკმაოდ მარტივად განსახორციელებელია. როგორც უკვე აღინიშნა, თაღლითობის ერთ-ერთი ყველაზე გავრცელებული ფორმა ფიშინგია, რომლის დროსაც თავდამსხმელი მოტყუებით ცდილობს მსხვერპლისგან პირადი ინფორმაციის მიღებას. აღნიშნული შეტევა უმეტესად მავნე ბმულებისა და ელ.ფოსტის შეტყობინებების გამოყენებით ხდება. აქედან გამომდინარე, სანამ პირად ინფორმაციას გააზიარებთ ნებისმიერ ვებ-გვერდზე, აუცილებელია, გადაამოწმოთ რამდენად ლეგიტიმურია პლატფორმა, რომელიც ჩვენგან გარკვეულ ინფორმაციას ითხოვს. გაითვალისწინეთ, რომ ლეგიტიმური ორგანიზაციები არასოდეს მოითხოვენ სენსიტიურ ინფორმაციას ელ.ფოსტისა და სატელეფონო ზარის გამოყენებით.

გარდა ფიშინგისა, მნიშვნელოვანია სხვა შემთხვევებზე ყურადღების გამახვილება. მაგალითად, შესაძლოა თავდამსხმელები სხვადასხვა კომპანიის სახელით დაგიკავშირდნენ და ამ ფორმით სცადონ თქვენგან გარკვეული ინფორმაციის მიღება. აღნიშნული კომუნიკაცია შეიძლება შედგეს როგორც სოციალური მედიის პლატფორმების, ასევე სხვადასხვა SMS საშუალებებით (მაგალითად Whatsapp, Viber და სხვ.). შესაბამისად, კიდევ ერთხელ უნდა აღინიშნოს, რომ სანამ ნებისმიერი სახის ინფორმაციას გავაზიარებთ, მაქსიმალურად უნდა გადავამოწმოთ გამომგზავნის ავთენტურობა.

ბავშვები და სოციალური ქსელები

სოციალური მედია მნიშვნელოვან როლს თამაშობს ბავშვებისა და მოზარდების განვითარების პროცესში. ბევრად გამარტივდა როგორც მნიშვნელოვანი ინფორმაციის მიღება, ასევე მისი გაზიარება. ბავშვებისა და მოზარდებისათვის სოციალური მედიის პლატფორმები თვითგამოხატვის, კომუნიკაციისა და სოციალური ურთიერთქმედების გზებს

წარმოადგენს. თუმცა, მათ თან ახლავთ უამრავი გამოწვევა და საფრთხე და ხშირად ბავშვები ყურადღებას არ აქცევენ მსგავს რისკებს. აქედან გამომდინარე მნიშვნელოვანია, მშობელი ხშირად ესაუბროს მათ აღნიშნულ საკითხებზე, რათა მოზარდები მაქსიმალური ყურადღებით მოეკიდონ ნებისმიერი სახის პირადი ინფორმაციის გაზიარებას და სოციალური მედიის პლატფორმების ზოგადი გამოყენების წესებს.

ხაზგასასმელია ის ფაქტიც, რომ აღნიშნული პლატფორმების გამოყენებით მეგობრების შეძენაც საკმაოდ მარტივია, თუმცა ამასაც უამრავი საფრთხე ახლავს თან. შესაძლოა ბოროტმოქმედმა პირმა გარკვეული ფსიქოლოგიური მანიპულაციის მეთოდები გამოიყენოს ბავშვების წინააღმდეგ, მათ შორის კიბერბულინგით, დაშინებით და ა.შ., რაც შემდგომ შესაძლოა სავალალო შედეგებით დასრულდეს. შესაბამისად, თუ ბავშვი/მოზარდი ერიდება მშობელთან საუბარს და არ სურს არანაირი სახის კომუნიკაცია აღნიშნულ თემაზე, აუცილებელია ქცევის შესწავლა და მიზეზის დადგენა, რათა არიდებულ იქნას მსგავსი ტიპის შემთხვევები.

კიბერბულინგი

კიბერბულინგი გულისხმობს სოციალური მედიის ან/და სხვადასხვა აპლიკაციის გამოყენებით, სხვების შევიწროებას, მუქარას ან/და დაშინებას. იგი განსაკუთრებით გავრცელებულია ბავშვებსა და მოზარდებში. შესაბამისად, მნიშვნელოვანია მათი ცნობიერების ამაღლება შემდგომში მსგავსი პრობლემის იდენტიფიცირებისა და აღმოფხვრის მიზნით. მაგალითად, თუ ისინი გახდებიან კიბერბულინგის მსხვერპლი, აუცილებლად უნდა მივიდნენ მშობელთან, მასწავლებელთან ან სხვა დამხმარე პირთან და შეატყობინონ ფაქტის შესახებ. გარდა ამისა, მათ უნდა იცოდნენ ისიც, რომ თუ დაინახავენ სხვა პირს, რომელიც არის სავარაუდოდ კიბერბულინგის მსხვერპლი, ეს არ ნიშნავს, რომ მათ თვალი უნდა დახუჭონ შემთხვევაზე; პირიქით, ისინი ანალოგიურად უნდა მოიქცნენ მსგავს შემთხვევაშიც.

მაქსიმალური ყურადღება მიაქციეთ ბავშვების ქცევაში ონლაინ შევიწროვების (კიბერბულინგის) ნიშნებს, როგორიცაა განწყობის უეცარი ცვლილება, სასკოლო დავალებების არშესრულება, სკოლაში წასვლაზე ხშირად უარის თქმა და ა.შ.

გარდა ჩამოთვლილი ფაქტორებისა, ერთ-ერთი ყველაზე ყურადსაღები და მნიშვნელოვანი ფაქტორია ბავშვთა წინააღმდეგ მიმართული სექსუალური ხასიათის დანაშაული სოციალური პლატფორმების გამოყენებით, რომელიც სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაულია. თუ რაიმე სახის ნიშანს ან/და მტკიცებულებას აღმოაჩენთ მსგასი ტიპის შემთხვევებზე, გთხოვთ, დაუყოვნებლივ აცნობოთ საქართველოს შინაგან საქმეთა სამინისტროს 112-ის საშუალებით. დამნაშავეებისგან ბავშვთა დაცვა ციფრულ სივრცეში კოლექტიური პასუხისმგებლობა და თითოეული მოქალაქის მოვალეობაა, ხოლო დროული მოქმედება ზრდის ეფექტურობას და შეუძლია თავიდან აგვარიდოს მსგავსი შემთხვევები და შემდგომი ზიანი.

სოციალური მედიის დაცვის საუკეთესო პრაქტიკა

ერთ-ერთი უმნიშვნელოვანესი ფაქტორი სოციალური მედიის დასაცავად, რა თქმა უნდა, რთული და უნიკალური პაროლის გამოყენებაა - იგი უნდა შედგებოდეს მინიმუმ 12 სიმბოლოსგან, პატარა და დიდი ასოებისგან, რიცხვებისა და სიმბოლოებისგან (!@#$). (მაგალითად, “Rtul1pAr0l1&@38-7!”). თუ თავდამსხმელი ფიშინგ შეტევის გამოყენებით პაროლს მოიპარავს და თქვენს ანგარიშზე შესვლას შეეცდება, აუცილებელია მას ე.წ. წინაღობად ორმაგი ავთენტიფიკაცია (2FA) დახვდეს, წინააღმდეგ შემთხვევაში, იგი თქვენს ანგარიშზე შესვლას უპრობლემოდ მოახერხებს, ხოლო ორმაგი ავთენტიფიკაციის არსებობის შემთხვევაში, აღნიშნული მცდელობა წარუმატებელი აღმოჩნდება.

ამასთან, აუცილებელია რეგულარულად შეამოწმოთ თქვენი სოციალური მედიის ანგარიშების კონფიდენციალურობა. უნდა აკონტროლოთ, ვის უზიარებთ პირად ინფორმაციასა და სიახლეებს, ვინაიდან აღნიშნული ინფორმაცია შესაძლოა თქვენს წინააღმდეგ გამოიყენონ კიბერდამნაშავეებმა. ყოველთვის გაითვალისწინეთ, რომ თქვენი პირადი ინფორმაციის დაცვა არ არის ერთჯერადი პროცესი.

რაც შეეხება ბმულებს, როგორც უკვე აღინიშნა, აუცილებელია ნებისმიერი სახის ბმული საეჭვოდ მიიჩნიოთ, ვინაიდან ყველაზე ხშირად სწორედ მავნე ბმულების გამოყენებით ხდება ინფორმაციის მოპარვა და ასევე სხვა სახის მავნე მოქმედებები მომხმარებლების წინააღმდეგ. ამავდროულად, უმნიშვნელოვანესია ყურადღება მიექცეს შემოკლებულ ბმულებსაც (მაგალითად, TinyURL, BitLy და ა.შ.), რადგან მათი გამოყენებით თავდამსხმელებს მარტივად შეუძლიათ რეალური ბმულის დამალვა და მომხმარებლების შეცდომაში შეყვანა.

გთავაზობთ ყველაზე გავრცელებული სოციალური მედიის პლატფორმების უსაფრთხოებას და რეკომენდაციებს, რომლებიც უნდა გაითვალისწინოთ მათი გამოყენებისას:

Linkedin გახლავთ სოციალური მედიის ტიპის პლატფორმა, რომელიც ძირითადად გამოიყენება სხვადასხვა დარგის პროფესიონალების ერთმანეთთან დასაკავშირებლად. მნიშვნელოვანია, იცოდეთ ის ძირითადი საფრთხეები და რეკომენდაციები, რაც მის გამოყენებას ახლავს თან.

Facebook და **Instagram** ერთ-ერთი ყველაზე გავრცელებული სოციალური მედიის პლატფორმებია მსოფლიოს მასშტაბით. მათი ძირითადი დანიშნულებაა ინფორმაციის, სურათების, ვიდეოებისა და ე.წ. პოსტების გაზიარება.

TikTok განსაკუთრებით პოპულარული სოციალური მედიის პლატფორმაა, რომელიც გამოიყენება მცირე ზომის ვიდეოების გასაზიარებლად, მათ შორის შეიძლება იყოს როგორც სახალისო და შემეცნებითი ხასიათის, ასევე მავნე ტიპის შინაარსის მქონე ვიდეოები.

ძირითადი საფრთხეები და რეკომენდაციები სოციალური ქსელების გამოყენებისას:

კონფიდენციალურობის შენარჩუნება - ყურადღება უნდა მიაქციოთ სხვადასხვა სახის პირადი მონაცემების განთავსებას. მაგალითად, აეროპორტში გადაღებული სურათი, სადაც პასპორტი და მასზე განთავსებული მონაცემები ჩანს, შესაძლოა გამოიყენონ კიბერდამნაშავეებმა სხვადასხვა შეტევის განსახორციელებლად. ფოტოს ან ვიდეოს გამოქვეყნებამდე ყოველთვის უნდა გადაამოწმოთ მათი შიგთავსი და დარწმუნდეთ, რომ ნამდვილად არ შეიცავს რაიმე სენსიტიურ ინფორმაციას.

ორმაგი ავთენტიფიკაცია (2FA) - გთხოვთ, დააყენოთ ორმაგი ავთენტიფიკაცია სოციალური ქსელების ანგარიშებზე, რათა თქვენი უსაფრთხოება მაქსიმალურად დაიცვათ.

სხვა მომხმარებლებთან დაკავშირება - სოციალურ ქსელებში მარტივია "მეგობრების" დამატება და უცხო ადამიანებთან დაკავშირება. მნიშვნელოვანია, დავრწმუნდეთ ამ ადამიანების ანგარიშების ავთენტურობაში, რადგან მათ წვდომა აქვთ თქვენს პირად ინფორმაციასთან.

ინტერნეტთაღლითობა - სოციალური ქსელები თაღლითობისათვის ერთ-ერთი ყველაზე მიმზიდველი საშუალებაა, ვინაიდან აქ უამრავი ადამიანი იყრის თავს, შესაბამისად მაქსიმალურად უნდა მოერიდოთ როგორც ბმულებზე გადასვლას, ასევე ნებისმიერი სახის ფაილის გადმოწერას.

ბავშვები სოციალურ ქსელებში - მნიშვნელოვანია, გააკონტროლოთ ბავშვების ანგარიშები და დარწმუნდეთ, რომ ისინი არ არიან კიბერბულინგის მსხვერპლნი და არ უწევთ მათთვის შეუსაბამო მასალის ნახვა.

მესამე მხარის აპლიკაციები (Third-Party Apps) - ხშირად სხვადასხვა აპლიკაციებში შესასვლელად გამოიყენება სოციალური მედიის პლატფორმები ავტომატური ავტორიზაციისთვის. მაგალითად თქვენი Facebook ანგარიშით შეიძლება დაუკავშირდეთ რომელიმე თამაშს. ეს იმას ნიშნავს, რომ ამ თამაშს აძლევთ უფლებას, მიიღოს, შეინახოს და გამოიყენოს თქვენი პირადი ინფორმაცია. შესაბამისად, ყურადღება უნდა მიაქციოთ, რა სახის აპლიკაციებს უკავშირდებით თქვენი ანგარიშიდან, რა ტიპისა და ოდენობის ინფორმაციას ინახავს და როგორ ამუშავებს ამ ინფორმაციას. არ დაეთანხმოთ წესებსა და პირობებს ავტომატურად, წაკითხვის გარეშე.

გასაჩივრება - სოციალური მედიის პლატფორმებს აქვთ გასაჩივრების (Reporting) ინსტრუმენტი. თუ შეხვდებით მავნე ხასიათის ვიდეოს ან სხვა ტიპის მასალას, შეატყობინეთ აღნიშნული სოციალური ქსელის ადმინისტრაციას, რათა დროულად აღმოფხვრან საკითხი.

თანამედროვე ციფრულ სამყაროში მობილური მოწყობილობების უსაფრთხოება კიბერჰიგიენის განუყოფელი ნაწილია. ამ თავში განიხილება სმარტფონების, ტაბლეტებისა და სხვა მობილური მოწყობილობების საფრთხეები, წესები და რეკომენდაციები, რომლებიც დაგეხმარებათ, დაიცვათ თქვენი პერსონალური ინფორმაცია კიბერდამნაშავეებისგან.

მობილური მოწყობილობების უსაფრთხოების მნიშვნელობა

სმარტფონი წარმოადგენს ყველაზე ხშირად გამოყენებულ მობილურ მოწყობილობას. მასში უამრავი პერსონალური ინფორმაცია იყრის თავს და შესაბამისად ის თაღლითებისთვის განსაკუთრებით მიმზიდველია. თუ კიბერდამნაშავე საკმარისი რაოდენობის პირად მონაცემებს მოიპოვებს, ის პოტენციურად შეძლებს თქვენი სახელით, მისამართით, პირადობის მოწმობის სურათებით გახსნას საბანკო ანგარიშები და განახორციელოს არაკანონიერი ტრანზაქციები; თქვენი სახელით აიღოს სესხები, დარეგისტრირდეს არასასურველ სერვისებზე, მოიპოვოს სხვა ანგარიშების პაროლები და უნებართვოდ გამოიყენოს თქვენი სოციალური ქსელები; მოიპოვოს წვდომა პირადი ცხოვრების ამსახველ მასალაზე და სცადოს შანტაჟის გზით ფულის გამოძალვა. მნიშვნელოვანია იცოდეთ, რა საფრთხეები და რისკები არსებობს რეალური სურათის წარმოდგენისა და შესაბამისი მზადყოფნის მიზნით.

მოძველებული სისტემა და აპლიკაციები

მობილურ მოწყობილობებში ორი ყველაზე გავრცელებული ოპერაციული სისტემა Android და IOS გვხვდება. მათი დეველოპერები პერიოდულად ახორციელებენ სისტემურ განახლებებს, რომლის მიზანიც შეიძლება იყოს ახალი ფუნქციონალის დამატება, ოპტიმიზაცია, ხარვეზების გამოსწორება და, რაც ყველაზე მნიშვნელოვანია, სისტემაში აღმოჩენილი სისუსტეების აღმოფხვრა. კიბერდამნაშავეები ცდილობენ მსგავსი სისუსტეები თავად იპოვონ, მათი გამოყენებით წვდომა მოიპოვონ მომხმარებლების მოწყობილობებზე და მოიპარონ პირადი ინფორმაცია.

იმისათვის, რომ შემცირდეს მსგავსი რისკი და საფრთხეები, საჭიროა, ხშირად შემოწმდეს მობილური მოწყობილობების სისტემები და რაც შეიძლება ადრე დაყენდეს შემოთავაზებული განახლებები. Android-ის და IOS-ის სისტემური განახლებების შემოწმება და სხვა დამატებითი ინფორმაციის მიღება

შესაძლებელია მოწყობილობის პარამეტრებში, როგორც წესი, “Software Update” ან “System Update” სექციაში.

არანაკლებ მნიშვნელოვანია ცალკეული აპლიკაციების განახლებაც. ანალოგიურად თქვენს მოწყობილობებში უამრავი პროგრამაა ჩაწერილი, სადაც ასევე პოულობენ სისუსტეებს და მათი აღმოფხვრის გარეშე აპლიკაციის გამოყენება გარკვეულ რისკებს წარმოქმნის. აპლიკაციების განახლების შემოწმება და დაყენება Android მოწყობილობებზე შესაძლებელია Play Store-ში, ხოლო IOS მოწყობილობებზე App Store-ში. პროცესის გასამარტივებლად შესაძლებელია პარამეტრებში ავტომატური განახლებების ჩართვაც.

მავნე აპლიკაციები

როგორც უკვე აღინიშნა, Android მოწყობილობებზე ახალი აპლიკაციების დაყენებისთვის ძირითადად Play Store გამოიყენება. მიუხედავად იმისა, რომ Play Store გუგლის ოფიციალური პლატფორმაა, მასზე მაინც იტვირთება მავნე პროგრამები, რომლებიც ძირითადად მომხმარებლის სენსიტიური ინფორმაციის მოპარვას ცდილობენ.

აღსანიშნავია, რომ ხშირად კიბერდამნაშავეები პოპულარული აპლიკაციების კლონებს ქმნიან მსგავსი სახელითა და გამოსახულებით. თუ აპლიკაცია საეჭვოდ გამოიყურება, საჭიროა გადმოწერამდე შემოწმდეს ავტორის გვერდი და თუ საჭირო გახდა დამატებითი ინფორმაციის მოძიებაც დეველოპერის სანდოობაში დარწმუნების მიზნით. მიუხედავად იმისა, რომ ყალბი შეფასებების დაგენერირებაც არ წარმოადგენს კიბერდამნაშავისთვის პრობლემას, მაინც რეკომენდებულია, აპლიკაციის მიმოხილვების შემოწმება, განსაკუთრებით კრიტიკული და უარყოფითი.

ზოგჯერ კიბერდამნაშავეები ქმნიან აპლიკაციას, გარკვეული დროის განმავლობაში მოიპოვებენ მომხმარებლების ნდობას და შემდეგ განახლების სახით აპლიკაციაში აგზავნიან მავნე კოდს. თუ საეჭვოა აპლიკაციის სანდოობა, ინსტალაციის ან განახლების შემდეგ შესაძლებელია მოწყობილობის პარამეტრებში შემოწმდეს აპლიკაციის ნებართვები და წვდომები კამერაზე, მიკროფონზე, ლოკაციაზე, კონტაქტებზე, მეხსიერებაზე, ხოლო შემდგომ აუცილებლად გამორთეთ ისეთი ჩართული პარამეტრები, რომლებიც არ არის საჭირო მათი ფინქციონირებისათვის. ამასთან, თუკი ესა თუ ის აპლიკაცია აღარ არის საჭირო, აუცილებლად უნდა წაიშალოს რისკების შემცირების მიზნით.

Android მოწყობილობებზე Play Store-ის გარდა აპლიკაციების დაყენება შესაძლებელია უცხო წყაროებიდან APK გაფართოების ფაილის გადმოწერით და მისი გაშვებით. Android Package Kit (APK) არის სპეციალურად Android-ის ოპერაციული სისტემისთვის შექმნილი დაარქივებული ფაილი, რომელიც აპლიკაციების ინსტალაციისთვისაა განკუთვნილი. მასში მავნე კოდის დამალვა მარტივია და არარეგულირებადი წყაროდან მისი გადმოწერა უსაფრთხოების რისკებს საგრძნობლად ზრდის.

IOS მოწყობილობებისთვის განკუთვნილ App Store-ზე მკაცრი პოლიტიკის გამო კიბერდამნაშავეებისთვის შედარებით რთულია მავნე აპლიკაციის ატვირთვა, თუმცა სიფრთხილის გამოჩენა ამ პლათფორმაზეც საჭიროა. ასევე IOS სისტემა მომხმარებლებს საკმაოდ ურთულებს უცხო წყაროებიდან აპლიკაციების ინსტალაციას, რაც ზოგჯერ არაკომფორტული, თუმცა დადებითი მხარეა უსაფრთხოების თვალსაზრისით.

მოწყობილობის დაბლოკვა - Screen lock

მობილური მოწყობილობის ეკრანის დაბლოკვა არის ყველაზე საბაზისო და აუცილებელი უსაფრთხოების

ფუნქციონალი, რომლის გარეშეც ნებისმიერ ადამიანს შეუძლია სმარტფონის გამოყენება და სენსიტიურ ინფორმაციაზე წვდომის მოპოვება. ამ ფუნქციონალის დაყენება და გამოყენება საკმაოდ მარტივია და, როგორც წესი, Android-ის სმარტფონებზე აუცილებელი პირობაცაა მას შემდეგ, რაც მომხმარებელი მოწყობილობას Google-ის ანგარიშს დაუკავშირებს.

არსებობს მოწყობილობის განბლოკვის სხვადასხვა მეთოდი, მათ შორისაა პაროლი, პინ კოდი, ეკრანზე დასახაზი ფიგურა (pattern), სახის ამოცნობა, თვალის გუგისა და ბადურის სკანერი, თითის ანაბეჭდი და სხვა. სხვადასხვა მწარმოებელი ამ მეთოდების განსხვავებულ კომბინაციებს გვთავაზობს. მნიშვნელოვანია, რომ შევარჩიოთ ძლიერი პაროლი ან გამოვიყენოთ ბიომეტრიული ავთენტიფიკაციის რომელიმე მეთოდი.

მოწყობილობის დაკარგვა და მოპარვა

მობილური მოწყობილობის დაკარგვის შემთხვევაში არსებობს რისკი, რომ უცხო პირი მოიპოვებს მეპატრონის პირად ინფორმაციაზე წვდომას და შეეცდება მის ბოროტად გამოყენებას. ამ დროს სწრაფი მოქმედება მეტად კრიტიკულია. საბედნიეროდ, ციფრული პორტალის საშუალებით შესაძლებელია დაკარგული Android და iOS მოწყობილობების მდებარეობის დადგენა. ამისათვის საჭიროა მოწყობილობებსა და ციფრულ, ინტერნეტთან დაკავშირებულ პორტალზეც ავტორიზებული იყოს შესაბამისად Google-ის ანდა iCloud ანგარიშები.

Android მოწყობილობებისთვის შეგვიძლია შევიდეთ შემდეგ ბმულზე: **google.com/android/find** ხოლო iOS მოწყობილობებისთვის შემდეგზე: **apple.com/lae/icloud/find-my**

გარდა ლოკაციის დადგენისა, ამ ონლაინ პორტალებიდან შეგვიძლია მოწყობილობის დაბლოკვა, ანგარიშებიდან გამოსვლა და მოწყობილობიდან ყველანაირი ინფორმაციის გასუფთავება. ამ უკანასკნელის შემთხვევაში ჩვენ დავკარგავთ მოწყობილობის მდებარეობაზე წვდომას.

აღსანიშნავია, რომ ამ ფუნქციონალის გამოყენებისთვის დაკარგული მოწყობილობა დაკავშირებული უნდა იყოს ინტერნეტთან ან ფიჭვური კავშირგაბმულობის სერვისთან.

Juice Jacking

კიდევ ერთი საფრთხე, რომელიც მობილურ მოწყობილობებს შეიძლება დაემართოს ცნობილია Juice Jacking-ის სახელით.

ამ დროს მომხმარებელი სმართფონის დასატენად იყენებს უცხო USB კაბელს, ან უცხო USB პორტს. სმარტფონები ელექტროენერგიის მისაღებად და მონაცემების გასაცვლელად ერთიდაიმავე კაბელს იყენებენ. ამის გამო დასატენად შეერთებულ კაბელს აქვს ინფორმაციის მოპარვის ან მოწყობილობაში მავნე კოდის ჩატვირთვის საშუალება. ეს მეთოდი განსაკუთრებით ხშირად გამოიყენება აეროპორტებში, სავაჭრო ცენტრებში და სხვა საჯარო სივრცეებში.

Juice Jacking-ისგან თავის დასაცავად თანამედროვე სმარტფონებს აქვთ ფუნქციონალი, რომელიც მომხმარებელს საშუალებას აძლევს აირჩიოს სასურველი რეჟიმი, გააგრძელოს მოწყობილობის დამუხტვა და დაბლოკოს მონაცემების მიმოცვლა. გარდა ამისა, არსებობს დამატებითი USB გადამყვანი (Data Blockers), რომლებიც ფიზიკურად ბლოკავენ მონაცემების მიმოცვლას.

SIM Hijacking - ტელეფონის ნომრის მიტაცება

კიბერდამნაშავეები ზოგჯერ თავიანთი მსხვერპლის წინააღმდეგ იყენებენ მეთოდს, რომელიც ცნობილია SIM Swapping-ის ან SIM Hijacking-ის სახელით. ამ დროს კიბერდამნაშავე ცდილობს, მსხვერპლის ტელეფონის ნომერი გადააპორტიროს ახალ SIM ბარათზე და წვდომა მოიპოვოს ნომერზე შემავალ ზარებსა და შეტყობინებებზე. ამისათვის ის უკავშირდება მსხვერპლის სერვისის პროვაიდერს და წინასწარ მოპოვებული პერსონალური ინფორმაციის ან/და ყალბი საიდენტიფიკაციო დოკუმენტების დახმარებით თავს ნომრის ნამდვილ მფლობელად ასაღებს. წარმატებული პორტირების შემდეგ კიბერდამნაშავის ხელში არსებულ SIM ბარათზე მსხვერპლის ნომერი აქტიურდება, ხოლო ორიგინალი SIM ბარათი უფუნქციო ხდება.

კიბერდამნაშავისთვის ამ პროცედურის სირთულე დამოკიდებულია იმაზე, თუ როგორი უსაფრთხოების ზომები აქვს სერვისის პროვაიდერს მიღებული,

როგორ ადასტურებს მომხმარებლის ვინაობას და რამდენად კვალიფიციური პერსონალი ჰყავს დაქირავებული.

მიტაცებული ნომრით კიბერდამნაშავეს შეუძლია მსხვერპლის მიერ დაყენებული მულტიფაქტორული ავთენტიფიკაციის გადალახვა (იხილეთ მე-3 თავი), რადგან ერთჯერადი დამადასტურებელი კოდები პირდაპირ მის SIM ბარათზე გაიგზავნება. შედეგად დამნაშავე შეძლებს მსხვერპლის პაროლების ანულირებას და ხელახლა შექმნას, რის შედეგადაც მოიპოვებს ანგარიშებზე წვდომას.

მსგავსი შეტევისგან თავის ასარიდებლად მნიშვნელოვანია, რომ არ გავაზიაროთ ზედმეტი პერსონალური ინფორმაცია ინტერნეტში და არ გავუმარტივოთ კიბერდამნაშავეებს ჩვენი თავის განსახიერება.

განუსაზღვრელი პრივილეგიების მოპოვება Android-ზე

ტერმინი "Rooting"ძირითადად ანდროიდის მოწყობილობების მიმართ გამოიყენება და გულისხმობს სისტემის root (მთავარ) საქაღალდეზე წვდომის მოპოვებას. შედეგად მომხმარებელს სისტემის სრული კონტროლის საშუალება ეძლევა. მისი დახმარებით შესაძლებელია მწარმოებლის მიერ ჩაშენებული შეზღუდვების გაუქმება და სისტემის მაქსიმალური მორგება მომხმარებლის სურვილებზე. iOS მოწყობილობებზე მსგავსი, თუმცა გაცილებით შეზღუდული პროცესი jailbreaking-ის სახელითაა ცნობილი. iOS სისტემაზე სრული კონტროლის მოპოვება შედარებით რთულია.

Rooting ლეგიტიმური ქმედების ფარგლებში მეტად გამოსადეგი პროცესია, თუმცა მას აქვს უარყოფითი მხარეებიც. მაგალითად, Rooting-ის შემდეგ რთულდება სისტემაზე განახლებების დაყენება, რაც ზრდის უსაფრთხოების

რისკებს, რადგან, როგორც ზემოთ ითქვა, მოძველებული პროგრამული უზრუნველყოფა კიბერშეტევების დროს მოწყვლადი და დაუცველია. ასეთი პრივილეგიების მოპოვების შემდეგ მოწყობილობა დაუცველია მავნე აპლიკაციების წინაშეც. მსგავს აპლიკაციას მარტივად შეუძლია სისტემის მნიშვნელოვანი ფაილების შეცვლა, უსაფრთხოების შეზღუდვების გადალახვა და კიბერდამნაშავის ჩანაფიქრების შესრულება. გარდა ამისა, ასეთ მოწყობილობებზე ზოგიერთი პროგრამა, განსაკუთრებით საბანკო აპლიკაციები, წყვეტს მუშაობას. ასევე, მათ უუქმდებათ გარანტია, რადგან ხშირ შემთხვევაში, Rooting პროცესი მწარმოებლის მიერ დადგენილი გამოყენების წესების დარღვევად ითვლება. ზოგჯერ Rooting-ის პროცესმა შეიძლება მოწყობილობა სრულიად გამოუსადეგარიც კი გახადოს.

მავნე QR კოდები - Quishing

QR (Quick Response) კოდები ხშირად ჩნდება საჯარო სივრცეებში, სარეკლამო ბანერებზე, გადახდის აპარატებთან და ა.შ. მათ გამოსაყენებლად საჭიროა სკანერი, რომელიც აპლიკაციებში ან თავად სმარტფონის კამერაშივე არის ჩაშენებული.

QR კოდში ძირითადად მცირე ზომის ტექსტური ინფორმაციაა შენახული და ყველაზე ხშირად ის ვებსაიტების ბმულებისთვის გამოიყენება. შესაბამისად, ყველა ის წესი და რეკომენდაცია, რომელსაც წინა თავებშია მოცემული ინტერნეტის უსაფრთხო გამოყენების შესახებ, ამ შემთხვევაშიც რელევანტური და გამოსადეგია. QR კოდის დასკანერებით და ბმულზე გადასვლით პერსონალური ინფორმაციის მოპარვის რისკი იზრდება.

საბედნიეროდ, უახლეს სკანერ აპლიკაციებსა და სმარტფონის კამერებს აქვს ფუნქციონალი, რომლის საშუალებითაც თვალსაჩინოა ვებ-საიტზე გადასვლამდე მისი მისამართი. შესაბამისად, მარტივდება პოტენციური ფიშინგ გვერდებისა და სხვა საფრთხის შემცველი ბმულების ამოცნობა.

სმიშინგი (Smishing), ვიშინგი (Vishing) და მობილური მესენჯერების უსაფრთხოება

სმიშინგი არის ფიშინგის ერთ-ერთი ნაირსახეობა და გულისხმობს თაღლითური SMS შეტყობინებების გაგზავნას მსხვერპლის ტელეფონის ნომერზე. როგორც წესი, თაღლითები თავს ასაღებენ რომელიმე სანდო და ცნობილ კომპანიად და მომხმარებელს მითითებულ ბმულზე გადასვლას სთხოვენ.

არსებობს SMS-ის გაგზავნის მეთოდები, რომლის საშუალებითაც თაღლითები ცვლიან გამგზავნის სახელს და ანაცვლებენ მას ნებისმიერი ტექსტით, მაგალითად ცნობილი კომპანიის, მსხვერპლის ნათესავის ან ოჯახის წევრის სახელით. მსგავსი შეტყობინებები დამაჯერებლად გამოიყურება და დაკვირვებას საჭიროებს.

ვიშინგის დროს კიბერდამნაშავეები მსხვერპლს პირდაპირ ურეკავენ და სოციალური ინჟინერიის ხრიკებით პერსონალური ინფორმაციის, მაგალითად, საბანკო რეკვიზიტების მიღებას ცდილობენ.

აღსანიშნავია, რომ ტელეფონის ნომერზე განხორციელებული ზარებითა და გაგზავნილი SMS შეტყობინებებით გაცილებით მეტის გაკეთებაა შესაძლებელი ვიდრე უბრალო სოციალური ინჟინერია. მაგალითად, ერთ-ერთი ყველაზე საშიში პროგრამა რომელიც Pegasus-ის სახელით არის ცნობილი გავრცელებული ინფორმაციის თანახმად იყენებს მავნე კოდის გავრცელების ისეთ ტექნიკას, როდესაც სმართფონზე შემოსული ზარი, უპასუხოდ დარჩენილიც კი, საკმარისია მობილური მოწყობილობის დასაინფიცირებლად. თუმცა მსგავსი პროგრამების შექმნა უდიდეს რესურსებთანაა დაკავშირებული და რა თქმა უნდა მისი მუშაობის დეტალები გასაიდუმლოებულია.

Bluesnarfing და Bluejacking

Bluetooth უკაბელო კომუნიკაციის ერთ-ერთი ფორმაა. ის ხშირად გამოიყენება მობილური მოწყობილობების

ერთმანეთთან დასაკავშირებლად. Bluetooth-ის უახლესი ვერსიები შედარებით დაცულია და მათი გამოყენება არ წარმოადგენს უსაფრთხოების რისკს. თუმცა მოწყობილობები, რომლებიც კვლავ იყენებენ Bluetooth-ის ძველ ვერსიებს, გაცილებით დაუცველია და მომხმარებელს პერსონალური ინფორმაციის მოპარვის რისკის ქვეშ აყენებს. კიბერდამნაშავეები იყენებენ ცნობილ სისუსტეს და ახლოს მყოფ მომხმარებლის მოწყობილობას შეუმჩნევლად უკავშირდებიან, რის შემდეგაც სმარტფონში შენახული ფოტოების, ვიდეოების, კონტაქტების და სხვა ფაილების გადმოწერის მოთხოვნებს აგზავნიან. შეტევის ამ მეთოდს Bluesnarfing ჰქვია.

Bluetooth-თან დაკავშირებული კიდევ ერთი შეტევის ფორმაა bluejacking. ამ დროს კიბერდამნაშავე ახლო მდებარე მოწყობილობებთან აგზავნის არასასურველ შეტყობინებებს ტექსტის ან სურათების სახით. ეს მეთოდი ანონიმურია და მსხვერპლთან მხოლოდ გამომგზავნის მოწყობილობის სახელი და მოდელის ნომერი ფიქსირდება. საბედნიეროდ ამ შეტევის დროს დამნაშავე ვერ ახერხებს თქვენს მონაცემებზე წვდომის მოპოვებას, თუმცა Bluetooth-ის ქსელში ხშირად გამოგზავნილი შეტყობინებები შეიძლება შემაწუხებელი იყოს და მოწყობილობის დატვირთვის მიზეზიც გახდეს.

მსგავსი თავდასხმებისგან თავის დასაცავად საჭიროა მობილური მოწყობილობების სისტემისა და აპლიკაციების რეგულარული განახლება. ყოველთვის გამორთეთ Bluetooth მაშინ და ჩართეთ მხოლოდ მისი გამოყენების დროს.

მონაცემთა კლასიფიკაცია

ინფორმაცია არის მონაცემთა ერთობლიობა, რომელიც სტრუქტურიზებულია, აქვს კონტექსტი, დამუშავებულია და შესაძლებელია მისი გადაცემა. მონაცემთა უსაფრთხოება არის ციფრული ინფორმაციის დაცვის პროცესი მისი მთელი სასიცოცხლო ციკლის განმავლობაში.

მონაცემთა დაცვის მიზნით, პირველ რიგში, საჭიროა მისი კლასიფიკაცია რესურსების სწორად გადანაწილებისა და სწორი უსაფრთხოების ზომების მიღებისთვის. მონაცემთა კლასიფიკაცია არის მონაცემების დაჯგუფების პროცესი მისი სენსიტიურობის დონის, რისკებისა და მათი შესაბამისი დაცვის წესების მიხედვით. არსებობს 3 ტიპის ინფორმაცია: საჯარო, შინასამსახურებრივი გამოყენების და კონფიდენციალური/აკრძალული.

საჯარო ინფორმაცია - ინფორმაცია, რომელიც შეიძლება საჯაროდ გაზიარდეს რისკების გარეშე. აქ არ მოიაზრება სენსიტიური ინფორმაცია, რომელიც განზრახ არის საჯაროდ ხელმისაწვდომი. მაგალითად: გენერალური ოფისის ტელეფონის ნომერი და ელ.ფოსტის მისამართი, საჯარო ვებგვერდის კონტენტი.

შინასამსახურებრივი გამოყენების ინფორმაცია - ეს არის ინფორმაცია, რომელიც გამოიყენება თანამშრომლებსა და სახელშეკრულებო ურთიერთობის მქონე პირებს შორის, სამსახურებრივი მოვალეობის შესრულების მიზნით და არ არის განკუთვნილი საჯაროდ გაზიარებისთვის. მაგალითად: კომპანიის შიდა პოლიტიკები და პროცედურები, თანამშრომელთა საკონტაქტო ინფორმაციები და ა.შ.

კონფიდენციალური ინფორმაცია - სენსიტიური ინფორმაცია, რომელზე წვდომაც მკაცრად არის განსაზღვრული და რომელიც დაცული უნდა იქნას არაავტორიზებული წვდომისაგან. მაგალითად: ფინანსური ჩანაწერები, მომხმარებლების პირადი მონაცემები, საკრედიტო ბარათები, პირადი ნომრები და ა.შ.

არსებობს ინფორმაციის მდგომარეობის სამი ტიპი:

Data at Rest - მონაცემები, რომლებიც ინახება ორგანიზაციაში;

Data in Transit - მონაცემები, რომლებიც უშუალოდ გადაცემის პროცესშია;

Data in Use - მონაცემები, რომლებიც აქტიურად გამოიყენება;

Data at Rest გულისხმობს მონაცემებს, რომლებიც შენახულია ნებისმიერი ტიპის მყარ დისკზე ან მეხსიერებაზე. რაიმე კონკრეტულ ადგილას. ეს მონაცემები არ გამოიყენება კონკრეტულ დროს. მაგალითად: მონაცემთა ბაზა, რომელიც ინახავს თანამშრომლების ინფორმაციას; მყარ დისკზე შენახული ფაილი, რომელიც არ გვაქვს გახსნილი და არ ვგზავნით.

Data in Use გულისხმობს მონაცემებს, რომლებიც კონკრეტული დროის მონაკვეთში არის გახსნილი ან დამუშავების პროცესშია. აქტიურად არის გამოყენებული კომპიუტერის ოპერატიული მეხსიერების მიერ (RAM). მაგალითად: მომხმარებელს გახსნილი აქვს დოკუმენტი და ცვლის ტექსტს; მონაცემები, რომლებსაც იყენებს დროის კონკრეტულ მონაკვეთში ჩართული პროგრამული უზრუნველყოფა, მაგალითად ბანკის გადახდის სისტემა ფინანსური მონაცემების დამუშავებისას.

Data in Transit გულისხმობს მონაცემებს, რომლებიც მიმოიცვლება ინტერნეტის გამოყენებით, აპლიკაციებს ან სისტემებს შორის. მაგალითად: შეტყობინების გაგზავნა ელ.ფოსტის გამოყენებით, მონაცემების გადაგზავნა ლოკალური კომპიუტერიდან ღრუბლოვან სისტემებში (Cloud).

მონაცემების ნებისმიერი მდგომარეობის დროს არსებობს იმის საშიშროება, რომ დაირღვეს ინფორმაციის კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა (CIA). შესაბამისად, თითოეულ მდგომარეობაში მონაცემს სჭირდება დაცვის მექანიზმები, რომლის ცოდნა და სწორი გამოყენება საჭიროა ყოველდღიურ საქმიანობაში უსაფრთხოებისა და კონფიდენციალურობის შესანარჩუნებლად. ერთ-ერთი მსგავსი დაცვის მექანიზმი არის მონაცემთა შიფრაცია. მონაცემთა შიფრაცია გვეხმარება ჩვენი სენსიტიური ინფორმაციის დაცვაში.

მონაცემთა შიფრაცია

მონაცემთა შიფრაცია არის მონაცემთა ტრანსფორმაციის პროცესი ისეთ ფორმაში, რომელიც კარგავს თავის პირვანდელ შინაარს და მისი აღდგენა შესაძლებელია მხოლოდ დეშიფრაციის გასაღების გამოყენებით. დაშიფრულ ინფორმაციას ეწოდება შიფროტექსტი (Ciphertext) და მისი წაკითხვა შეუძლებელია დეშიფრაციის გარეშე.

მონაცემთა შიფრაცია გამოიყენება არასასურველი პირების მიერ ინფორმაციის წაკითხვისგან თავის არიდების მიზნით. მისი გამოყენება შეიძლება ნებისმიერი ტიპის მონაცემზე, რომელთა უსაფრთხოებაც მნიშვნელოვანია. მონაცემთა შიფრაციისათვის გამოიყენება შიფრაციის ალგორითმები, რომელთა გატეხვაც თეორიულად შესაძლებელია, თუმცა სჭირდება ძალიან დიდი დრო და ბევრი რესურსი.

დღესდღეისობით გამოიყენება შიფრაციის ორი ძირითადი ტიპი: **სიმეტრიული და ასიმეტრიული.** სიმეტრიული შიფრაციის დროს გამოიყენება ერთი საიდუმლო გასაღები (Secret Key) როგორც მონაცემთა შიფრაციისთვის, ასევე მისი დეშიფრაციისთვის, რაც გულისხმობს იმას, რომ ინფორმაციის გამგზავნიც და მიმღებიც სარგებლობს ერთი გასაღებით. შიფრაციის ეს ტიპი ძირითადად გამოიყენება დიდი ზომის ინფორმაციის მიმოცვლის დროს.

ასიმეტრიული შიფრაცია, მეორენაირად საჯარო გასაღების შიფრაცია (Public Key Cryptography) იყენებს ორ ერთმანეთთან დაკავშირებულ გასაღებს, საჯაროს და პირადს (Public and Private). საჯარო გასაღები არის ყველასთვის ხელმისაწვდომი და გამოიყენება ინფორმაციის დასაშიფრად, ხოლო პირადი გასაღები არის შენახული მხოლოდ იმ პირთან, ვინც უნდა მიიღოს ეს ინფორმაცია და მხოლოდ ამ პირადი გასაღების საშუალებით ხდება დეშიფრაცია.

ორივე მათგანს გააჩნია თავისი დადებითი და უარყოფითი მხარეები. სიმეტრიული შიფრაცია არის უფრო სწრაფი სხვა ტიპის შიფრაციებთან შედარებით, რადგან ის იყენებს ერთ გასაღებს როგორც შიფრაციისათვის ასევე დეშიფრაციისათვის. შესაბამისად არის უფრო ეფექტიანი, მოიხმარს ნაკლებ რესურსებს და შეიძლება ფული და დრო დაზოგოს. სიმეტრიული შიფრაცია არის გამოსაყენებლად მარტივი და სწორედ ამიტომ არის იგი პოპულარული. გარდა ამისა, სიმეტრიული შიფრაცია არის თავსებადი ძალიან ბევრ ფართოდ გამოყენებულ პროგრამულ უზრუნველყოფებთან (Software, Hardware), რაც ნიშნავს იმას რომ მისი ინტეგრაცია ბევრი წვალების გარეშეა შესაძლებელი იმ აპლიკაციებში, რომლებსაც უკვე ყოველდღიურად იყენებთ. ასიმეტრიული შიფრაცია არის უფრო უსაფრთხო და აქვს უფრო ძლიერი შიფრაციის მექანიზმი. ამას განაპირობებს ის ფაქტი, რომ პირადი (Private) გასაღები აქვს მხოლოდ ინფორმაციის მიმღებს და სხვა მის გარდა ვერ

შეძლებს მონაცემების დეშიფრაციას, მათ შორის ვერც ის პიროვნება, ვინც თავად დაშიფრა ინფორმაცია. ასიმეტრიული შიფრაციის გასაღების გაზიარებისათვის არ არის საჭირო დაცული გზების გამოყენება, რადგან საჯარო გასაღები ყველასთვის ხელმისაწვდომია და ყველა ადამიანს თავისი საჯარო-პირადი (Public-Private key pair) გასაღებების წყვილი უნდა ჰქონდეს. ეს ამარტივებს ამ ტიპის შიფრაციის გამოყენებას. სიმეტრიული შიფრაციის მსგავსად, ასიმეტრიული შიფრაციაც არის თავსებადი ბევრ ფართოდ გამოყენებულ პროგრამულ უზრუნველყოფებთან. საბოლოოდ, სიმეტრიული შიფრაცია არის უფრო სწრაფი და მარტივად გამოსაყენებლი, მაგრამ ნაკლებად უსაფრთხო ასიმეტრიულ შიფრაციასთან შედარებით. ასიმეტრიული არის მეტად დაცული, მაგრამ ნელი და რთულად დასანერგი.

ყველაფრის მიუხედავად, მაინც არსებობს შეტევის ტიპები, რომელთა მეშვეობითაც ჰაკერები ცდილობენ ამა თუ იმ შიფრების გატეხვას. ყველაზე ცნობილი და ხშირად გამოყენებადი ასეთი შეტევის ტიპი გახლავთ Brute-Force, რომლის საშუალებითაც შემტევები ცდილობენ გატეხონ/გამოიცნონ შიფრაციის გასაღები შემთხვევითი სიმბოლოების ცდით. რაც უფრო დიდია გასაღები ზომაში, მით უფრო რთულია მსგავსი ტიპის შეტევით მისი გატეხვა; მაგრამ რაც უფრო დიდია გასაღების ზომა, მით უფრო მეტი კომპიუტერის რესურსი სჭირდება მის გამოყენებას.

არსებობს ერთ-ერთი Microsoft-ის სერვისი, რომელიც Microsoft-მა 2006 წელს შეიმუშავა და Windows Vista-დან მოყოლებული ყველა Windows-ზე გვხვდება. BitLocker არის მყარი დისკის შიფრაციის ხელსაწყო, რომლის საშუალებითაც ხელმიუწვდომელს ხდის დისკზე არსებულ ფაილებს არაავტორიზებული პირებისაგან. მაგალითად, თუ უცხო პირს ჩაუვარდება ხელში ლეპტოპი ან მყარი დისკი, Windows სისტემაზე პაროლის არსებობის მიუხედავად, შესაძლებელია მისი გვერდის ავლა არაერთი ხერხით და მასზე არსებული ყველა ფაილი ხელმისაწვდომი გახდება ამ პირისათვის. BitLocker-ის გამოყენებით კი მონაცემები დაიშიფრება და სისტემის პაროლის გვერდის ავლის შემთხვევაშიც შეუძლებელია თქვენი მონაცემების მოპარვა. გამომდინარე იქიდან, რომ BitLocker ძალიან მარტივად გამოყენებადია ყველასთვის, ის ძალიან ხშირად გამოიყენება როგორც ინდივიდუალური პიროვნებების, ისე დიდი ორგანიზაციების მიერ.

როგორც სხვა ყველა თავდაცვის მექანიზმი, BitLocker-იც რათქმაუნდა 100%-იან უსაფრთხოების გარანტიას არ წარმოადგენს, ყოფილა შემთხვევები როდესაც შემტევებმა მოახერხეს BitLocker-ის შიფრაციის გვერდის ავლა, ამიტომაც არის საჭირო სხვა უსაფრთხოების მექანიზმების არსებობაც.

მონაცემების შიფრაცია აუცილებელია მაშინაც, როდესაც მონაცემები მოძრაობის ფაზაშია (Data in Transit), რისთვისაც საჭიროა უსაფრთხო კომუნიკაციის პროტოკოლების გამოყენება,

რომლებიც უზრუნველყოფს ინფორმაციის კონფიდენციალურობას, მთლიანობას და ხელმისაწვდომობას. ყველაზე ხშირად გამოყენებადი პროტოკოლი შიფრაციისათვის არის SSL/TLS, Secure Socket Layer/Transport Layer Security. ეს პროტოკოლი ამყარებს უსაფრთხო, დაშიფრულ კავშირს სერვერსა და კლიენტს შორის, რაც ნიშნავს იმას რომ შიფრავს ყველა იმ მონაცემს, რომელიც მოძრაობს სერვერსა და კლიენტს შორის. SSL/TLS გამოიყენება ვებ აპლიკაციებში, ელექტრონულ ფოსტებში და სხვა სერვისებში რომელიც იყენებს HTTP პროტოკოლს.

PGP ანუ Pretty Good Privacy არის ერთ-ერთი პირველი საჯაროდ ხელიმისაწვდომი ასიმეტრიული შიფრაციის სისტემა, რომელიც პირველად 1991 წელს შეიქმნა Paul Zimmerman - ის მიერ. PGP ძირითადად გამოიყენება ელექტრონული ფოსტით ინფორმაციის მიმოცვლის უსაფრთხოებისათვის. ეს სისტემა იყენებს ასიმეტრიულ შიფრაციას, რაც ნიშნავს იმას რომ მონაცემები იშიფრება საჯარო გასაღების საშუალებით (Public key). როდესაც ერთი პიროვნება მეორეს უგზავნის შეტყობინებას ელ.ფოსტის გამოყენებით, ეს შეტყობინება იშიფრება მეორე პიროვნების საჯარო გასაღებით და საბოლოოდ მიმღები ამ ინფორმაციას განშიფრავს თავისი პირადი გასაღებით (Private Key).

Gpg4win არის უფასო პროგრამული უზრუნველყოფა, რომლის საშუალებითაც მარტივად შეიძლება მონაცემების დაშიფრვა და შემდეგ უკვე დაშიფრულის გაზიარება სხვა პირებთან. მისი გადმოწერა შესაძლებელია ოფიციალური ვებგვერდიდან https://www.gpg4win.org/. მოცემული პროგრამული უზრუნველყოფა არის სრულიად უფასო, თუმცა დეველოპერები იღებენ დონაციებს სურვილის შემთხვევაში, ან 0$ ის მითითების შემთხვევაში უფასოდ გადმოწეროთ gpg4win.

მონაცემთა გასუფთავება (Data erasure)

სენსიტიური ინფორმაციის შენახვა კომპიუტერში არ არის რეკომენდებული, მას შემდეგ რაც ინფორმაცია აღარ არის საჭირო - ის უნდა წაიშალოს სისტემიდან. თუმცა, სისტემიდან როცა იშლება ფაილი, რეალურად იშლება ამ ფაილის მისამართი, ფაილი კი კვლავ რჩება სისტემაში; ამ ფაილის აღდგენა შესაძლებელია მანამ, სანამ მას სხვა რაიმე არ გადაეწერება ზედ. მონაცემების გასასუფთავებლად აუცილებელია მასზე

შემთხვევითად დაგენერირებული ციფრების გადაწერა, რადგან მისი აღდგენა შეუძლებელი გახდეს. ამისათვის არსებობს რამოდენიმე უფასო ხელსაწყო, როგორიცაა მაგალითად shred, Secure Erase, WipeFile და Sdelete, Sdelete Microsoft - ის მიერ შექმნილი Sysinternals-ის პროგრამული უზრუნველყოფაა.

WipeFile არის უფასო, პორტატული პროგრამული უზრუნველყოფა, რომლის გამოყენება შეგიძლიათ დაინსტალირების გარეშე. პროგრამის გახსნის შემდეგ ვირჩევთ ფაილს, ფაილებს ან მთლიანად ფოლდერს რომლის გასუფთავებაც გვსურს. შემდეგ მარცხენა დაბალ კუთხეში ვირჩევთ Wipe-ს და ჩვენი მონაცემები სისტემიდან წაშლილია მთლიანად, ანუ მის ადგილას სხვა ამ პროგრამული უზრუნველყოფის მიერ გენერირებული მონაცემები იწერება, რაც თითქმის შეუძლებელს ხდის პირვანდელი ინფორმაციის აღდგენას.

სარეზერვო ასლები (Backup)

სარეზერვო ასლი, იგივე Backup გულისხმობს მონაცემების ასლების გადატანას მეორე, განსხვავებულ ლოკაციაზე შენახვის მიზნით. ეს შეიძლება ეხებოდეს ნებისმიერი სახის მონაცემს, მაგალითად: დოკუმენტებს, ფოტოსურათებს, მთლიან მონაცემთა ბაზებს ან საერთოდ მთლიან სისტემებს. სარეზერვო ასლების ქონა, არის კრიტიკულად მნიშვნელოვანი. მონაცემების დაკარგვა შეიძლება მოხდეს ძალიან ბევრი მიზეზით. მაგალითად: Ransomware შეტევით, სისტემის დაქრაშვით, შემთხვევითი წაშლით ან უბრალოდ ბუნებრივი კატასტროფით (ხანძარი, წყალდიდობა, მიწისძვრა და ა.შ.). ხშირ შემთხვევაში, კრიტიკული ინფორმაციის დაკარგვა ბიზნესისათვის ან თუნდაც კერძო პირისათვის შეიძლება დიდი ზიანის მომტანი იყოს. სარეზერვო ასლების ქონის შემთხვევაში, ნებისმიერი ზემოთ ჩამოთვლილის დროსაც კი, შესაძლებელია დაკარგულ მონაცემებზე წვდომის დაბრუნება.

სარეზერვო ასლების ასაღებად არსებობს ე.წ. 3-2-1 წესი უსაფრთხოებისათვის, რომლის მიხედვითაც, მონაცემების მინიმუმ 3 ასლი უნდა არსებობდეს, მინიმუმ 2 ასლი უნდა იყოს შენახული ფიზიკურად სხვა დისკზე, ხოლო მინიმუმ 1 ასლი უნდა იყოს შენახული ფიზიკურად სხვა ლოკაციაზე.

“Backup” შეიძლება გაკეთდეს როგორც ავტომატურად, მაგალითად კვირაში ერთხელ, ასევე ხელით, სურვილისამებრ. დროთა განმავლობაში უფრო და უფრო პოპულარული ხდება ქლაუდ სერვისების გამოყენება სარეზერვო ასლების შესანახად. მაგალითად: OneDrive, Dropbox და ა.შ.

OneDrive არის ერთ-ერთი ყველაზე ხშირად გამოყენებადი არჩევანი მონაცემთა ასლებისთვის. მისი საშუალებით შესაძლებელია ფაილების სარეზერვო ასლების ავტომატური შექმნა და ღრუბლოვან პლატფორმებზე მოთავსება, Microsoft-ის ანგარიშზე.

უმთავრესი პრობლემა არის ის, რომ უფასო ვერსიაზე არის ლიმიტი და მაქსიმუმ 5 GB მონაცემების ატვირთვაა შესაძლებელი.

სამუშაო გარემოს უსაფრთხოება

კიბერუსაფრთხოებაში ციფრულ სივრცესთან ერთად მნიშვნელოვანია ფიზიკური თავდაცვის მექანიზმების უზრუნველყოფაც. ოფისში ნებისმიერმა მცირე შეცდომამაც კი შეიძლება გამოიწვიოს ისეთი მნიშვნელოვანი ზიანი, როგორიცაა კომპანიის ან/და თანამშრომლებისა და მოხმარებლების სენსიტიური ინფორმაციის გაჟონვა, პიროვნების ქურდობა, ფინანსური სარგებელი და მრავალი სხვა. შესაბამისად, მნიშვნელოვანია, თითოეულმა პირმა აიღოს პასუხისმგებლობა საკუთარ თავზე და დაიცვას კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის პრინციპები.

უპირველესად, ყველაზე ხშირი უსაფრთხოების რისკი გახლავთ სამუშაო მაგიდაზე კომპიუტერთან ნებისმიერი სახის ჩასანიშნი ფურცლების გამოყენება, რომელზეც შეიძლება არსებობდეს სენსიტიური ან პირადი ინფორმაცია. უფრო კონკრეტულად, პატარა ფურცელი შეიძლება შეიცავდეს მომხმარებლის პაროლებს, საფოსტო მისამართდებს ან შიდა ინფორმაციას. არასასურველი პირის მიერ ამ ინფორმაციის წაკითხვა დიდ რისკს წარმოადგენს, ამიტომაც ფიზიკური ფურცლების მაგივრად რეკომენდებულია პაროლების მენეჯერის გამოყენება, ხოლო სხვადასხვა საკითხების ჩასანიშნად - "sticky notes" რომელიც თითქმის ყველა თანამედროვე ოპერაციულ სისტემაში გვხვდება.

მეორე მნიშვნელოვანი საკითხია კომპიუტერის ეკრანის დაბლოკვა მაშინ, როცა მისი მეპატრონე არ იყენებს და მის სიახლოვეს არ არის. კომპიუტერის დაბლოკვის გარეშე დატოვება იგივეა, რაც სახლიდან გასვლა და კარების ღიად დატოვება. ასეთ

დროს ნებისმიერს შეუძლია, ნახოს თქვენს კომპიუტერში

არსებული ფაილები, გამოიყენოს ელექტრონული ფოსტა, ნახოს პაროლები, ან სულ რამდენიმე წამში დააინსტალირონ მავნე კოდის შემცველი პროგრამა. მიზანი შეიძლება იყოს როგორც პირადი ინტერესი ან შურისძიება, ისე კონკრეტული ორგანიზაციის მიმართ მავნე აქტივობის განხორციელება. კომპიუტერის ეკრანის დასაბლოკად შეგიძლიათ, გამოიყენოთ კლავიატურაზე Windows-ის ნიშანისა და L ასო-ბგერის კომბინაცია.

ბოლო პერიოდში ორგანიზაციებმა უფრო მეტად დაიწყეს ციფრული ტრანსფორმაცია. ისინი თანამშრომლებს სთავაზობენ მეტად მოქნილ სამუშაო გარემოს საკუთარი სახლებიდან. ამ დროს კი როგორც ფიზიკური, ასევე ციფრული ასპექტების დაცვა კიდევ უფრო გადამწყვეტი ხდება. აღსანიშნავია ის ფაქტიც, რომ ორგანიზაციებს ხშირად უჭირთ უსაფრთხოების დონის მართვა და კონტროლი, როდესაც თანამშრომლები დისტანციურად მუშაობენ. პირველ რიგში უნდა გესმოდეთ და გაითავისოთ , რატომ არის აუცილებელი დისტანციურად მუშაობის დროს კიბერუსაფრთხოების ზომების მიღება.

სენსიტიური ინფორმაციის დაცვა - დისტანციურად მუშაობის დროს, ორგანიზაციისთვის სენსიტიური ინფორმაცია ხშირად ზიარდება სახლში არსებულ პერსონალურ მოწყობილობებსა და ქსელში. რეკომდენირებული კიბერუსაფრთხოების ზომების გათვალისწინების გარეშე ეს მონაცემები დაუცველი ხდება.

არ გადმოწეროთ პირატული პროგრამები - უმეტეს შემთხვევაში ასეთი პროგრამები შეიცავს მავნე კოდს, რამაც შეიძლება თქვენს კომპიუტერზე მოახდინოს არაავტორიზებული წვდომის მოპოვება.

არ გადახვიდეთ საეჭვო ბმულებზე !

IoT მოწყობილობები

Internet of Things (**IoT),** იგივე ნივთების ინტერნეტი არის ერთგვარი მოწყობილობები (მაგალითად სენსორები , გაჯეტები და ა.შ.), რომლებიც დაპროგრამებულია გარკვეულ აპლიკაციებში და შეუძლიათ მონაცემთა გადაცემა ინტერნეტით. ამჟამინდელი მონაცემებით, დაფიქსირებულია 112 მილიონზე მეტი კიბერშეტევა IoT დევაისებზე და ეს

მაჩვენებელი დღითიდღე იზრდება. ამ ყველაფრის გამომწვევი მიზეზებია ავტომატურად დაყენებული, სუსტი, ადვილად გამოსაცნობი პაროლები. ასევე მოძველებული და გასანახლებელი სისტემური დონის პროგრამული უზრუნველყოფა ე.წ. Firmware, რომელიც უზრუნველყოფს სპეციფიკური მოწყობილობების გამართვას. შესაბამისად, დისტანციურად მუშაობის დროს ეს თითქოს და უწყინარი გარემოებები შეიძლება გახდეს თქვენი მოწყობილობების ექსპლუატაციისა და შემდგომ თქვენი კორპორაციების მოწყვლადობის მიზეზი.

IoT - დევაისების უმეტესობა მოწყვლადია, რადგან მათ არ აქვთ ისეთი უსაფრთხოების მექანიზმები, როგორებიც გვხვდება ოპერაციულ სისტემებზე. ისინი შექმნილია გარკვეული დავალებების შესასრულებლად და მაგ ფუნქციონალის გამართვაზეა ორიენტაცია გაკეთებული. ასევე მათი უმეტესობა არ იყენებს ძლიერი შიფრაციის ალგორითმებს, რის გამოც ქსელში ინფორმაციის მიმოცვლის დროს ეს დევაისები მოწყვლადები არიან Person In The Middle შეტევებისას. ამ რისკების შესამცირებლად საჭიროა, ასეთი დევაისები ამოფარებული იყოს Firewall-ის უკან და მასში გამავალი ტრაფიკის მონიტორინგი ხდებოდეს.

აუცილებლად გამოიყენეთ უსაფრთხო და განახლებული პროგრამული უზრუნველყოფა, ასევე კომპიუტერისა და მობილური ტელეფონის საოპერაციო სისტემები.

სახლის შიდა ქსელის უსაფრთხოება

დაიცავით თქვენი WIFI როუტერი ძლიერი და უნიკალური პაროლით , ასევე თავი აარიდეთ მის გაზიარებას მაგალითად მეზობლებთან ან უცხო პირებთან. ასევე დარწმუნდით , რომ თქვენი როუტერი იყენებს ძლიერი დაშიფვრის ალგორითმებს WPA2 & WPA3.

WPA2 - არის დაშიფრული უსაფრთხოების პროტოკოლი , რომელიც იცავს ინტერნეტ ტრაფიკს უსადენო ქსელებში. WPA2 - Wi-Fi Protected Access უსადენო ქსელების უსაფრთხოების პროტოკოლის მეორე თაობა, რომელიც გთავაზობთ სანდო და ძლიერ შიფრაციას.

WPA3 - არის WPA2 ის განახლებული ვერსია , რომელიც გვთავაზობს მეტად გაძლიერებულ შიფრაციას. WPA2 - ისგან განსხვავებით , რომელიც იყენებდა ყველა მოწყობილობაზე ერთ **encryption keys** , WPA3 ყველა დაკავშირებული დევაისისთვის იყენებს სხვადასხვა უნიკალურ **encryption keys. Encryption Key -** არის ერთგვარი გასაღები , რომლის მეშვეობითაც მონაცემების დაშიფვრა და გაშიფვრა.

თქვენივე უსაფრთხოებისთვის რეკომენდირებულია სახლში არ ჰქონდეთ მოძველებული როუტერები რადგან როუტერის დაჰაკვის შემთხვევაში კიბერ დამნაშავეებს თქვენ ქსელზე და ქსელზე ჩართულ მოწყობილობებზე სრული კონტროლის საშუალება ეძლევათ.

Person-In-The-Middle - შეტევები

მიყურადების შეტევა გულისხმობს არასანქცირებული გზით ორი მოწყობილობის კომუნიკაციაში მესამე პირის ჩარევას. შეტევის წარმატებულად განხორციელების შემთხვევაში, მესამე პირს შესაძლებლობა ეძლევა გაფილტრული ან შეცვლილი ინფორმაცია მიაწოდოს სამიზნე სისტემას. Person-In-The-Middle შეტევის განხორციელების შესაძლებლობა კიბერდამნაშავეს მაშინ ეძლევა, როცა მას აქვს წვდომა თქვენს შიდა ქსელზე. ასეთი შეტევების თავიდან ასარიდებლად საჭიროა გამოიყენოთ ყოველთვის უსაფრთხო კომუნიკაციის გზა ბრაუზერსა და სერვერს შორის HTTPS. ასევე მიზანშეწონილი იქნება დამატებითი უსაფრთხოების მიზნით თუ გამოიყენებთ VPN-ს, რომელიც სრულად დაშიფრავს თქვენს ტრაფიკს.

Evil Twin Attack

Evil-Twin Attack - ხდება მაშინ, როდესაც თავდამსხმელი ქმნის ყალბ Wi-Fi ქსელს და ახდენს თქვენი Wi-Fi-ს კლონირებას, იმ იმედით რომ მომხმარებლები დაუკავშირდებიან მას ლეგიმიტური Wi-Fi-ს ნაცვლად. როდესაც მსხვერპლი ასეთ მავნე Wi-Fi-ს დაუკავშირდება, კიბერდამნაშავეებს უჩნდებათ შესაძლებლობა განახორციელონ სხვადასხვა ტიპის შეტევები. გადმოაწერინონ მსხვერპლს მავნე პროგრამა ან გადაამისამართონ ლეგიტიმური საიტების ნაცვლად ფიშინგ ბმულებზე. მოისმინონ ქსელში გამავალი ტრაფიკი სრულიად.

VPN - Virtual Private Network

VPN-ის გამოყენება დისტანციურად მუშაობის დროს კრიტიკულად მნიშვნელოვანია, ის მუშაობის დროს უსაფრთხოების ერთ-ერთი გარანტია და საგრძნობლად ამცირებს სხვადასხვა კიბერ-შეტევების რისკს. მისი გამოყენების დროს Person-In-The-Middle-ის შეტევების რისკი ნულს უტოლდება. ასევე ჩვენი რეალური IP მისამართი დამალულია და IP-Based შეტევების რისკს საგრძნობლად ვამცირებთ. ასევე VPN-ის ერთ-ერთი მთავარი დადებითი მხარე არის ის,რომ ჩვენი ტრაფიკი არის დაშიფრული, შესაბამისად მესამე მხარე(ISP) ვერ შეძლებს ჩვენი ტრაფიკის მოსმენას და მონიტორინგს (იხ. დეტალურად მე-5 თავში).

ონლაინ შეხვედრები

დისტანციურად მუშაობის დროს ხშირად გვიწევს ჩავერთოთ სხვადასხვა ტიპის ონლაინ შეხვედრებს მაგალითად zoom-ში ან სხვა ნებისმიერ პლატფორმაზე. თავდამსხმელებმა

შეიძლება გამოიყენონ ასეთი პლატფორმები თავიანთი მავნე მიზნებისთვის. არსებობს სხვადასხვა ტიპის შეტევები ამ პლატფორმების გამოყენებით , მაგალითად Zoom-bombing . სოციალური ინჟინერიის ან თუნდაც საჯარო ფორუმებიდან დასასწრები ბმულის მოპოვების შემდგომ , ისინი უერთდებიან ონლაინ შეხვედრებს და ცდილობენ გამოიწვიონ ქაოსი. ასეთი მომენტების თავიდან ასაცილებლად საჭიროა, ნებისმიერი ონლაინ შეხვედრა არ აქვს მნიშვნელობა რომელ პლატფორმაზე იქნება, აღჭურვილი იყოს ძლიერი პაროლით . ასევე თავი შეიკავეთ ასეთი ბმულების საჯარო ფორუმებზე გაზიარებით. აცნობეთ მონაწილეებს უცნობ ბმულებზე დაწკაპუნების რისკებზე და შეხვედრის მოწვევის წყაროს გადამოწმების მნიშვნელობის შესახებ.

ჯანდაცვის მსოფლიო ორგანიზაცია ახალი სუპერვირუსის გამო საგანგებო მდგომარეობას აცხადებს "

ოფიციალური წყაროები იუწყებიან, რომ ჯანდაცვის მსოფლიო ორგანიზაციამ (WHO) გამოაცხადა გლობალური საგანგებო მდგომარეობა ახალი ვირუსის “COVID-24” მოულოდნელი გამოჩენის გამო, რომელიც ცნობილია, რომ უფრო გადამდები და მომაკვდინებელია ვიდრე COVID-19. ორგანიზაციასთან დაახლოებული წყაროები ირწმუნებიან, რომ ამ ვირუსს, რომელიც სავარაუდოდ წარმოიშვა ინდოეთში, აქვს პოტენციალი გლობალურად გავრცელდეს რამდენიმე დღეში, 50%-ზე მეტი სიკვდილიანობის მაჩვენებლით. ჯერჯერობით არ არსებობს ვაქცინა ან რაიმე სახის სამკურნალო საშუალება ვირუსისაგან დასაცავად.

რატომ არის ეს კურსი მნიშვნელოვანი? წარმოვიდგინოთ, რომ ზემოაღნიშნული ახალი ამბავი ვრცელდება სოციალურ ქსელებში, ტელევიზიებსა და რადიოში, რა იქნებოდა თქვენი რექცია?

ზემოხსენებული ახალი ამბები მთლიანად გამოგონილია, შექმნილია საგანმანათლებლო მიზნებისთვის და ის გვიჩვენებს, თუ რამდენად ადვილად შეუძლია ყალბ ამბებს, რომ გააჩინოს შიში და დაბნეულობა. ამ თავში განვიხილავთ ინსტრუმენტებსა და საშუალებებს, რომლებიც აუცილებელია ამგვარი დეზინფორმაციის

იდენტიფიცირებისთვის და წინააღმდეგობის გასაწევად, ხაზს ვუსვამთ მედიაწიგნიერების კრიტიკულ საჭიროებას ჩვენს სულ უფრო ციფრულ სამყაროში.

დღევანდელ ციფრულ სამყაროში, სადაც თითოეულ ადამიანს აქვს საინფორმაციო ტექნოლოგიებზე, მობილურ მოწყობილობებსა და ინტერნეტზე წვდომა, დეზინფორმაციის შექმნა და გავრცელება ბევრად უფრო მარტივი გახდა ვიდრე ამის შესაძლებლობა აქამდე არსებობდა. გასათვალისწინებელია ის გარემოება, რომ საქართველოსთან მიმართებით დეზინფორმაცია სულ უფრო მეტად მნიშვნელოვანი ხდება იმ გარემოების გათვალისწინებით, რომ ხდება საქართველოს ევროკავშირთან დაახლოება და შესაბამისად უცხოური და არაკეთილმოსურნე ქვეყნები ცდილობენ გავლენა მოახდინონ და ევროკავშირის ღირებულებები წარმოაჩინონ არასწორ კონტექსტში.

დეზინფორმაციისა და მისინფორმაციის საფუძვლები

დღევანდელ ციფრულ ეპოქაში, სადაც ინფორმაცია უფრო სწრაფად გადაიცემა ვიდრე ოდესმე, ნამდვილი და ცრუ ინფორმაციის გარჩევის უნარი გადამწყვეტი გახდა. დეზინფორმაცია და მისინფორმაცია მნიშვნელოვან გავლენას ახდენენ საზოგადოებაზე. მათ შეუძლიათ დაამახინჯონ საზოგადოებრივი აზრი და განწყობა, გავლენა მოახდინონ პოლიტიკურ პროცესებზე და საფრთხე შეუქმნან საზოგადოებრივ ჯანდაცვას. ყალბი ამბების გავრცელებამ შეიძლება გავლენა მოახდინოს არჩევნებზე, შექმნას ჯანმრთელობასთან დაკავშირებული მითები, რომლებიც ვირუსულად ვრცელდება ინტერნეტ სივრცეში, რამაც შეიძლება საფრთხე შეუქმნას ადამიანის სიცოცხლეს. ციფრული პლატფორმების განვითარებასთან ერთად, ასევე ვითარდება ყალბი ინფორმაციის გავრცელების მეთოდები, რაც კიდევ უფრო ართულებს და ამავდროულად მნიშვნელოვანს ხდის დეზინფორმაციასთან ბრძოლას.

ჩვენ ასევე განვიხილავთ სტრატეგიებსა და ინსტრუმენტებს, რომლებიც ხელმისაწვდომია ამ ფენომენებთან საბრძოლველად. ცრუ ინფორმაციის ეფექტურად ამოცნობის, ანალიზისა და მასთან ბრძოლის მიზნით, თქვენ გაეცნობით კრიტიკული აზროვნების მეთოდებს, ტექნოლოგიების გამოყენებასა და რეალური შემთხვევების კრიტიკულ ანალიზს. დეზინფორმაციისა და მისინფორმაციის იდენტიფიცირებისა და ბრძოლის უნარის გაძლიერებით, შეგიძლიათ მნიშვნელოვანი როლი შეასრულოთ უფრო ღია, გამჭვირვალე და სანდო საინფორმაციო გარემოს ჩამოყალიბებაში.

დეზინფორმაციისა და მისინფორმაციის არსი

დეზინფორმაცია გულისხმობს ინფორმაციას, რომელიც განზრახ შექმნილი ან შეცვლილია სხვების მოტყუების ან შეცდომაში შეყვანის მიზნით. ის ხშირად მიზნად ისახავს ზიანის მიყენებას საზოგადოებრივ აზრზე ან ქცევაზე მავნე ზეგავლენის მოხდენას. დეზინფორმაცია არ არის მხოლოდ არასწორი ინფორმაცია; ის შეგნებულად შექმნილია მავნე მიზნებისთვის, მისი სამიზნე შეიძლება იყოს ინდივიდები, ჯგუფები, ორგანიზაციები ანდა ქვეყანა.

დეზინფორმაციის მაგალითი: *სარეკლამო სააგენტო რეპუტაციის შელახვისა და ამომრჩევლებზე ზემოქმედების მიზნით, ქმნის ყალბ ახალ ამბებს იმის მტკიცებით, რომ პოლიტიკური ოპონენტი ჩართულია უკანონო ქმედებებში.*

მისინფორმაცია პირიქით, გულისხმობს ცრუ ინფორმაციის გაზიარებას, მაგრამ მოტყუების განზრახვის გარეშე. ხშირად, ეს არის გაუგებრობის, შეცდომის ან უცოდინრობის შედეგი. მისინფორმაცია არ არის შექმნილი მავნე განზრახვით, მაგრამ მაინც შეიძლება გამოიწვიოს დაბნეულობა და გაუგებრობა საზოგადოებაში.

მაგალითი: *ადამიანი აზიარებს პოსტს სოციალურ მედიაში, სადაც ნათქვამია, რომ ლეღვის ფოთლის წვენის რეგულარული მოხმარება იწვევს კანის კიბოს განკურნებას. სინამდვილეში, ეს ინფორმაცია არაზუსტია და პოტენციურად შეცდომაში შემყვანი, მაგრამ პირს ვინც აზიარებს შესაძლოა მიაჩნდეს, რომ ეს სიმართლეა და ის არ აპირებს სხვების მოტყუებას; ის თავად არის მისინფორმირებული.*

ამ ორის ერთმანეთისგან განასხვავებლად, გასათვალისწინებელია მთავარი ფაქტორი - განზრახვა. დეზინფორმაცია ვრცელდება **მოტყუების მიზნით**, ხოლო მისინფორმაცია შეიძლება გავრცელდეს **გაუგებრობის ან არასწორი კომუნიკაციის გამო**.

დეზინფორმაციის რეალური მაგალითი:

2016 წლის შეერთებული შტატების საპრეზიდენტო არჩევნებში იყო დეზინფორმაციის შემთხვევები, ერთ-ერთი თვალსაჩინო მაგალითია "პიცაგეიტის" შეთქმულების თეორია. ეს სრულიად უსაფუძვლო თეორია ამტკიცებდა, რომ დემოკრატიული პარტიის მაღალჩინოსნები მონაწილეობდნენ ბავშვთა სექსის რინგში, რომელიც მოქმედებდა ვაშინგტონში, პიცის რესტორანში. შეთქმულების შედეგად რესტორანში გასროლაც კი მოხდა.

მისინფორმაციასთან დაკავშირებული რეალური შემთხვევები:

2018 წელს, ინდოეთში WhatsApp-ზე გავრცელებულმა ცრუ ჭორებმა გამოიწვია ადამიანთა ლინჩის წესით გასამართლება. აპლიკაციის საშუალებით გავრცელდა დეზინფორმაცია ბავშვთა გამტაცებლებთან დაკავშირებით, რამაც გამოიწვია პანიკა და რამდენიმე ადამიანის ტრაგიკული სიკვდილი, რომლებიც შეცდომით მიიჩნეოდნენ გამტაცებლებად.

ჯანმრთელობასთან დაკავშირებული მისინფორმაციის რეალური მაგალითები:

ვაქცინაციის საწინააღმდეგო მოძრაობა, განსაკუთრებით 1998 წელს ენდრიუ უეიკფილდის მიერ გამოქვეყნებული დისკრედიტირებული კვლევის შედეგად, ცრუდ აკავშირებდა წითელას, ყბაყურასა და წითურას (MMR) ვაქცინას აუტიზმთან. ამ დეზინფორმაციამ გამოიწვია ვაქცინაციის მაჩვენებლის შემცირება და ამ დაავადებების შემდგომი აფეთქებები მსოფლიოს სხვადასხვა კუთხეში.

თანამედროვე მაგალითი: *COVID-19 პანდემიის დროს, დეზინფორმაციის მნიშვნელოვანი ნაწილი იყო ჰიდროქსიქლოროქინის პოპულარიზაცია, როგორც ვირუსის სამკურნალო საშუალება. მიუხედავად სამედიცინო კვლევების არ არსებობისა, რეკლამაში ასევე ჩართულები იყვნენ გავლენიანი ფიგურები და პოლიტიკოსები. ყოველივე ამან, გამოიწვია პრეპარატზე მოთხოვნის ზრდა, და საბოლოოდ, მედიკამენტების ბოროტად გამოყენება, რაც უარყოფით გავლენას ახდენდა მომხმარებელზე. ასევე დეფიციტის გამო პრობლემა შეექმნათ მათაც ვისაც ეს წამალი რეალურად სჭირდებოდა.*

გავლენა საზოგადოებაზე:

დეზინფორმაცია და მისინფორმაცია, მიუხედავად იმისა, რომ განსხვავებულია მათი განზრახვები, ორივე მნიშვნელოვან გავლენას ახდენს საზოგადოებაზე. მათ შეუძლიათ გავლენა მოახდინონ საზოგადოებრივ აზრზე, ჯანმრთელობის შედეგებსა და დემოკრატიულ პროცესებზე. მოდით, უფრო დეტალურად განვიხილოთ ეს ზემოქმედება:

გავლენა საზოგადოებრივ აზრზე:

დეზინფორმაცია: მიზანმიმართულად ცრუ ინფორმაციის გავრცელებამ შეიძლება შექმნას ან გაამწვავოს სოციალური განხეთქილება, რაც სხვადასხვა ჯგუფებს შორის მტრობასა და უნდობლობას იწვევს. მაგალითად, პოლიტიკურ კონტექსტში დეზინფორმაციის კამპანიებმა შეიძლება მოახდინონ პოლარიზაცია პოლიტიკურ, ანდა საზოგადოებრივ ჯგუფებს შორის, რაც იწვევს დაძაბულობასა და სოციალური თანხვედრის შემცირებას.

მისინფორმაცია: ბოროტი განზრახვის გარეშე გაზიარებულ ცრუ ინფორმაციას ასევე შეუძლია დაამახინჯოს კრიტიკული საკითხების მიმართ საზოგადოების გაგება და აღქმა. მაგალითად, გარემოსდაცვითი საკითხების შესახებ მისინფორმაციამ შეიძლება გამოიწვიოს საზოგადოების აპათია ან სკეპტიციზმი ისეთი პრობლემების თაობაზე, როგორიცაა კლიმატის ცვლილება.

გავლენა საზოგადოებრივ ჯანდაცვაზე:

დეზინფორმაცია: ჯანმრთელობის შესახებ ინფორმაციის განზრახ შეცდომაში შეყვანამ შეიძლება მძიმე შედეგები გამოიწვიოს. მაგალითია ცრუ ინფორმაციების განზრახ გავრცელება ვაქცინის საფრთხეების შესახებ, რაც იწვევს ვაქცინაციის მაჩვენებლის შემცირებასა და თავიდან აცილებადი დაავადებების გავრცელებას.

მისინფორმაცია: ჯანმრთელობის შესახებ ინფორმაციის არასწორად გაგებამ და გავრცელებამ, მაგალითად საოჯახო და ტრადიციული სამკურნალო საშუალებების გამოყენებით თვითმკურნალობამ, შეიძლება გამოიწვიოს ჯანმრთელობისთვის მავნე შედეგები, დაგვიანებული მკურნალობა ან ეფექტური სამედიცინო რჩევების უგულებელყოფა.

დემოკრატიულ პროცესებზე გავლენა:

დეზინფორმაცია: დეზინფორმაციის გამოყენება საარჩევნო შედეგებზე გავლენის მოხდენისთვის, როგორც ეს გლობალურად სხვადასხვა არჩევნებში ჩანს, ძირს უთხრის დემოკრატიული პროცესების მთლიანობას. მას შეუძლია გავლენა მოახდინოს არჩევნებზე, მანიპულაცია მოახდინოს ამომრჩეველთა არჩევანზე და დაარღვიოს დემოკრატიული ინსტიტუტებისადმი ნდობა.

მისინფორმაცია: მავნე განზრახვის გარეშეც კი, ხმის მიცემის პროცედურების, თარიღების ან კანდიდატის პოლიტიკის შესახებ არასწორი ინფორმაციის გავრცელებამ, შეიძლება შეაფერხოს დემოკრატიული პროცესი. ამან შეიძლება გამოიწვიოს ამომრჩეველთა დაბნეულობა, ამომრჩეველთა აქტივობის ჩახშობა და კითხვები არჩევნების შედეგების ლეგიტიმურობის შესახებ.

რეკომენდაციები დეზინფორმაციისა და მისინფორმაციისაგან თავის დასაცავად

გადაამოწმეთ ინფორმაციის წყაროები:

ყოველთვის შეამოწმეთ ინფორმაციის წყაროს სანდოობა. მოძებნეთ მიკერძოების მტკიცებულება ან არასწორი ანგარიშგების ჩანაწერი.

გამოიყენეთ ფაქტების შემოწმების ვებსაიტები ახალი ამბების დასადასტურებლად. (მაგალითად: Hoaxy, The Iffy Quotient, Lead Stories FactChecker, Information Operations Archive)

შინაარსის კრიტიკული ანალიზი:

კრიტიკულად გააანალიზეთ შინაარსი. ფრთხილად იყავით სენსაციური სათაურების ან ისტორიების მიმართ, რომლებიც ძლიერ ემოციურ რეაქციას იწვევს.

მოძებნეთ ლოგიკური შეცდომები ან გადაუმოწმებელი განცხადებები შინაარსის ფარგლებში.

ინფორმაციის ჯვარედინი შემოწმება:

ჯვარედინად გადაამოწმე სიახლეები მრავალ სანდო წყაროსთან. თუ ამბავი სიმართლეს შეესაბამება, ის სავარაუდოდ რამდენიმე სანდო საინფორმაციო გამოშვების მიერ იქნება მოხსენებული.

ფრთხილად იყავით სოციალურ მედიაში მკაფიო წყაროების გარეშე გავრცელებული ინფორმაციის.

საკუთარი თავისა და სხვების განათლება:

იყავით ინფორმირებული დეზინფორმაციისა და მისინფორმაციის კამპანიებში გამოყენებული საერთო ტაქტიკის შესახებ.

გაუზიარეთ თქვენი ცოდნა სხვებს, დაეხმარეთ მათ ამოიცნონ და თავიდან აირიდონ ცრუ ინფორმაციის გავრცელება.

მოერიდეთ გადაუმოწმებელი ინფორმაციის გაზიარებას:

თავი შეიკავეთ ახალი ამბების ან ისტორიების გაზიარებისგან, რომლებიც არ გაქვთ გადამოწმებული, განსაკუთრებით თუ ისინი შექმნილია საზოგადოების გაღვივების ან გაყოფის მიზნით.

წაახალისეთ სხვები, რომ გადაამოწმონ ინფორმაცია სანამ გააზიარებენ.

გამოიყენეთ ციფრული წიგნიერების ინსტრუმენტები:

გამოიყენეთ ციფრული ხელსაწყოები და ბრაუზერის გაფართოებები, რომლებიც ხელს უწყობენ ყალბი ამბებისა და საეჭვო წყაროების იდენტიფიცირებას. (მაგალითად: NewsGuard, Media Bias Fact Checker, Stopaganda Plus)

ჩაერთეთ ონლაინ პლატფორმებში, რომლებიც ხელს უწყობენ ზუსტი ინფორმაციის გავრცელებას.

დაარეპორტეთ საეჭვო ინფორმაცია:

დაარეპორტეთ ინფორმაცია იმავე პლატფორმაზე სადაც იპოვეთ, თუ ის ჩანს, რომ დეზინფორმაცია ან მისინფორმაციაა.

მონაწილეობა მიიღეთ საზოგადოების ძალისხმევაში, რათა შეეწინააღმდეგოთ ცრუ ინფორმაციის გავრცელებას.

იყავი სკეპტიკური იმ ინფორმაციის მიმართ, რომელიც „ზედმეტად კარგია, რომ სიმართლე იყოს“:

იყავით განსაკუთრებით სკეპტიკურად განწყობილი იმ განცხადებების მიმართ, რომლებიც შესანიშნავად შეესაბამება თქვენს უკვე არსებულ რწმენას ან ძალიან სენსაციური ან ცალმხრივი ჩანს.

გამოიკვლიეთ პოპულარული ამბების ფონი ან ინფორმაცია, მათი წარმოშობის გასაგებად.

ღია დიალოგისა და ურთიერთგაგების ხელშეწყობა:

ჩაერთეთ ღია დისკუსიებში საკამათო თემებზე, წაახალისეთ გაგების კულტურა და არა კონფლიქტი.

პატივი ეცით განსხვავებულ მოსაზრებებს და გამოიყენეთ ეს საუბრები, როგორც ფაქტების შემოწმებისა და განათლების შესაძლებლობები.

მოკლედ რომ ვთქვათ, დეზინფორმაციამ და მისინფორმაციამ შეიძლება ღრმა და პოტენციურად საზიანო გავლენა მოახდინონ საზოგადოებაზე. მათ შეუძლიათ შეარყიონ ინფორმირებული გადაწყვეტილების მიღება, დაარღვიონ ნდობა ინსტიტუტების მიმართ და გამოიწვიონ რეალური შედეგები, რომლებიც გავლენას ახდენენ ინდივიდებსა და საზოგადოებაზე. მნიშვნელოვანია, რომ ინდივიდებმა, მთავრობებმა და ორგანიზაციებმა ხელი შეუწყონ ციფრულ წიგნიერებასა და ფაქტების შემოწმებას ამ ეფექტების შესამცირებლად.