როგორ დავიცვათ ციფრული უსაფრთხოება - სრული გზამკვლევი ნინო გამისონიასგან

ონლაინ ანგარიშების დაცვა

როგორ მუშაობს ინტერნეტი

მნიშვნელოვანი ინფორმაციის კომპიუტერებზე, სმარტფონებსა თუ პლანშეტებზე შენახვისას, ადვილი არ არის იმის კონტროლი, თუ სად მიდის ეს მონაცემები. რაც უფრო მეტი თქვენი მოწყობილობაა დაკავშირებული ინტერნეტთან და რაც უფრო მეტი ინფორმაცია ინახება მესამე პირებთან და არა ადგილობრივად, მით უფრო რთულია მისი დაცვა დამნაშავეებისა და ჯაშუშობისგან.

- ინტერნეტი არის დეცენტრალიზებული ქსელი, რომელშიც არის ფიზიკური ინფრასტრუქტურა - სერვერი კომპიუტერები, კონტინენტთაშორისი წყალქვეშა კაბელები და მარშრუტიზატორები, რომლებიც, ძირითადად, მსხვილ კომპანიებს ეკუთვნით.
- შესაბამისად, არ არსებობს ისეთი ცნება, როგორიცაა „ღრუბელი“. არსებობენ მხოლოდ სხვა ადამიანების (ან კომპანიების) კომპიუტერები. როდესაც აპლიკაციის ან ვებსაიტის საშუალებით ტვირთავთ ან აზიარებთ შეტყობინებებს ან ფაილებს ინტერნეტით, საკუთარ თავს ჰკითხეთ:

✓ ვის კომპიუტერებს ან ინფრასტრუქტურას ვიყენებ?

✓ ვინ არის ამ პორგრამის მომწოდებელი?

✓ როგორია ბიზნეს მოდელი?

✓ ვენდობი თუ არა იმ ადამიანებს, რომელთა ინფრასტრუქტურასაც მე ვიყენებ?

შეაფასეთ თქვენი საფრთხის დონე

ციფრული უსაფრთხოება არ ეხება მხოლოდ იმას, თუ რომელ ინსტრუმენტებს/პროგრამებს იყენებთ. ეს არის იმის გაგება, თუ რა საფრთხეების წინაშე დგახართ და როგორ შეგიძლიათ, დაუპირისპირდეთ ამ საფრთხეებს. თქვენ უნდა განსაზღვროთ, რისი დაცვა გჭირდებათ და ვისგანაა დაცვა საჭირო.

- თქვენი მონაცემებისთვის საფრთხის შესაფასებლად საკუთარ თავს დაუსვით შემდეგი კითხვები:

✓ რისი დაცვა გსურთ?

✓ ვისგან გსურთ მისი დაცვა?

✓ რამდენად სავარაუდოა, რომ დაგჭირდეთ მისი დაცვა? (მაგალითად, რამდენად სავარაუდოა, რომ თქვენი რომელიმე მოწყობილობა შეიძლება მოიპარონ ან დაიკარგოს სადმე ტრანსპორტში ან კაფეში?)

✓ რამდენად ცუდი შედეგები შეიძლება მოჰყვეს, თუ მის დაცვას ვერ მოახერხებთ? (მაგალითად, რა მოხდება, თუ თქვენი შიდა ოფისის კომუნიკაცია გაჟონავს საჯაროდ, ან თუ მავნე განზრახვის მქონე პირმა მოიპოვა კონტროლი თქვენს Facebook ანგარიშზე?)

- ამ კითხვებზე პასუხები განსხვავდება ადამიანიდან ადამიანამდე და სხვადასხვა სიტუაციაში სხვადასხვანაირია; ისინი ასევე შეიძლება შეიცვალოს დროთა განმავლობაში. ამიტომ ღირს ამ სავარჯიშოს ხელახლა გამეორება პერიოდულად და საკუთარი თავის შემოწმება.

გამოიყენეთ ძლიერი პაროლები

პაროლები არის დაცვის პირველი ხაზი თქვენი მონაცემებისა და კომუნიკაციების დასაცავად. ისინი იცავენ თქვენს ონლაინ ანგარიშებსა და მონაცემებს, რომლებიც ადგილობრივად ინახება, მაგალითად ლოკალურ მყარ დისკზე ან USB მეხსიერებაზე. ძლიერი პაროლების გამოყენება თქვენთვის ნომერ პირველი პრიორიტეტი უნდა იყოს.

• ძლიერი პაროლი შედგება მინიმუმ 15 სიმბოლოსგან, შეიცავს სრულიად შემთხვევით არჩეულ დიდ და პატარა ასოებს, რიცხვებსა და სიმბოლოებს.

• ეს ნიშნავს, რომ ძლიერი პაროლები არ უნდა შეიცავდეს თქვენთან დაკავშირებულ პერსონალურ ინფორმაციას: თქვენს დაბადების თარიღს ან თქვენი მშობლიური ქალაქის სახელს, მეგობრების, ოჯახის წევრების ან საყვარელი შინაური ცხოველების სახელებს.

• არ უნდა გამოიყენოთ პაროლი ერთზე მეტი ონლაინ ანგარიშისთვის. ყველა ანგარიში დაცული უნდა იყოს საკუთარი უნიკალური პაროლით.

• პაროლები არ უნდა იყოს შენახული სხვაგან, გარდა პაროლის მენეჯერისა. არ ჩაწეროთ ისინი Word ან Excel ფაილებში, თუნდაც ეს ფაილები პაროლით იყოს დაცული. არც სამაგიდო ბლოკნოტში.

გამოიყენეთ პაროლის მენეჯერი

იმის გამო, რომ ძლიერი პაროლების შესახებ ზემოაღნიშნული წესების პრაქტიკაში განხორციელება რიგითი ადამიანებისთვის ურთულესი დავალებაა.

ყოველდღიური ცხოვრება, საქმიანობა და პაროლებთან ურთიერთობა უფრო მარტივი რომ გახდეს, თქვენ უნდა გამოიყენოთ პაროლის მენეჯერი.

პაროლის მენეჯერები პატარა პროგრამები ან აპლიკაციებია, რომლებიც საშუალებას მოგცემთ, უსაფრთხოდ შეინახოთ იმდენი პაროლი, რამდენიც გსურთ, ოღონდ დაიცავით ისინი ყველაზე სუპერ ძლიერი საპაროლო ფრაზით. ეს საშუალებას გაძლევთ, გქონდეთ ათობით ან თუნდაც ასობით სხვადასხვა ძალიან ძლიერი და უნიკალური პაროლი ყველა თქვენი ანგარიშისთვის.

• ერთ-ერთი ყველაზე ადვილად გამოსაყენებელი, ღია კოდის მქონე, უფასო პაროლის მენეჯერი არის Bitwarden. მისი გამოყენება შეგიძლიათ, როგორც ბრაუზერის დანამატი (ყველა ცნობილი ბრაუზერისთვის) ან როგორც დამოუკიდებელი აპლიკაცია კომპიუტერისთვის, Mac-ისთვის, Android-ისთვის და iPhone-ისთვის.

• Bitwarden ინახავს თქვენს ყველა პაროლს დაშიფრულ მონაცემთა ბაზაში და ავტომატურად ასინქრონებს მათ თქვენს მოწყობილობებს შორის. ამიტომ, ძალიან მნიშვნელოვანია თქვენი Bitwarden-ის ანგარიშის დაცვა ძალიან ძლიერი საპაროლო ფრაზით.

• ბაზარზე ასევე ხელმისაწვდომია სხვა პაროლის მენეჯერები, როგორიცაა 1password, Passbolt, Dashlane და ა.შ.

გააქტიურეთ ორეტაპიანი ავტორიზაცია, სადაც შესაძლებელია

ბევრი ონლაინ სერვისი, როგორიცაა Bitwarden, Google, Facebook, Twitter, Instargram, Microsoft და სხვები, შესაძლებლობას გაძლევთ, დაიცვათ თქვენი ანგარიში ორეტაპიანი ავტორიზაციით (2FA). ჩართეთ ეს ფუნქციან სადაც კი ეს შესაძლებელია, რადგან ის დაიცავს თქვენს ანგარიშებს მაშინაც კი, თუ ვინმემ თქვენი პაროლი მოიპარა.

• თქვენს სმარტფონზე დააინსტალირეთ FreeOTP აპი (Android და iPhone) ან Google Authenticator აპლიკაცია (Android და iPhone). შემდეგ გადადით ინტერნეტის პარამეტრების ან კონფიგურაციის დიალოგზე ანგარიშში, რომლისთვისაც გსურთ გააქტიუროთ ორეტაპიანი ავტორიზაცია და მიჰყევით ინსტრუქციას იქ. ჩვეულებრივ, ეს მოიცავს FreeOTP ან Google Authenticator აპის გახსნას QR კოდის სკანირებისთვის, რომელსაც თქვენი ონლაინ ანგარიში წარმოგიდგენთ.

• გააქტიურების შემდეგ, თქვენი ჩვეულებრივი მომხმარებლის სახელითა და პაროლით შესვლის შემდეგ, ონლაინ სერვისი მოგთხოვთ, შეიყვანოთ უნიკალური ერთჯერადი კოდი. ეს კოდი შექმნილია თქვენთვის FreeOTP ან Google Authenticator აპში და ჩვეულებრივ, მოქმედებს მხოლოდ ნახევარი წუთის განმავლობაში.

პაროლის აღდგენის უსაფრთხო მექანიზმები

ბევრი ონლაინ ანგარიშის პროვაიდერი, როგორიცაა ელ.ფოსტის ან ღრუბლოვანი საცავის პროვაიდერები, გთავაზობთ თქვენი პაროლის აღდგენას იმ შემთხვევაში, თუ ისინი დაგავიწყდათ. ზოგჯერ, ეს მოითხოვს პასუხის გაცემას წინასწარ განსაზღვრულ ეგრეთ წოდებულ „უსაფრთხოების კითხვებზე“. ზოგჯერ, პროვაიდერი უბრალოდ გიგზავნით ელ.წერილს პაროლის აღსადგენი ლინკით. „უსაფრთხოების კითხვები“ ყველაზე ცუდია საშუალებაა. ორივე შემთხვევა ქმნის უზარმაზარ ხარვეზს უსაფრთხოების თვალსაზრისით.

თუ თავდამსხმელმა თქვენს ელ.ფოსტის ანგარიშზე წვდომა მოიპოვა, რომელზედაც აღდგენის ბმულები იგზავნება, ეს მათ საშუალებას მისცემს მასობრივად შეცვალოს თქვენი სხვა ანგარიშების პაროლები, რომელზეც ესა თუ ის ელ.ფოსტა გაქვთ მიბმული.

• შეამოწმეთ, აქვს თუ არა თქვენს ყველაზე მნიშვნელოვან ონლაინ ანგარიშებს პაროლის აღდგენის ფუნქცია. თუ შესაძლებელია, გამორთეთ ეს ფუნქცია.

• სადაც ონლაინ ანგარიშმა დაგისვათ უსაფრთხოების კითხვები, როგორიცაა - „რა ჰქვია ჩემს ცხოველს?“ ან „რა არის დედაჩემის ქალიშვილობის სახელი?“, შეცვალეთ თქვენი პასუხები შემთხვევითი პაროლებით, რომლებიც შეგიძლიათ შეინახოთ თქვენი პაროლის მენეჯერში.

• ნებისმიერ შემთხვევაში: მოეპყარით ელ.ფოსტის ანგარიშს, რომელიც დაკავშირებულია თქვენს სხვა ანგარიშებთან (მაგ. Facebook, Twitter და ა.შ.) ძალიან ფრთხილად, დაიცავით იგი ძლიერი პაროლით და ორეტაპიანი ავტორიზაციით, როგორც ეს ზემოთ იყო ახსნილი. ამასთან, მოახდინეთ ელ.ფოსტის მისამართების დივერსიფიცირება - გამოიყენეთ სხვადასხვა ელ.ფოსტის მისამართი სხვადასხვა ანგარიშზე.

ინტერნეტის უსაფრთხოდ დათვალიერება და დაცვა ფიშინგის შეტევებისგან

აირჩიეთ კარგი ბრაუზერი

• ბრაუზერი თქვენი ფანჯარაა ინტერნეტში. ბაზარზე ბევრი ბრაუზერია, მაგრამ ყველა არ ითვალისწინებს მომხმარებლის საუკეთესო ინტერესს. იმიტომ, რომ ვინც აკონტროლებს ბრაუზერს, ასევე აკონტროლბს, თუ როგორ იყენებენ ადამიანები ვებ გვერდებს და შეუძლიათ მათი მართვა საკუთარი (კომერციული) მიზნებისთვის.

• ამიტომ, საუკეთესო ბრაუზერი არის ის, რომელსაც არ აკონტროლებს სარეკლამო კომპანია ან სხვა მარკეტინგული კომპანია, რომელსაც კომერციული ინტერესები გააჩნია.

• Firefox ბრაუზერი შექმნილია არაკომერციული Mozilla Foundation-ის მიერ, რომლის მისიაა ინტერნეტი ღია და ყველასთვის ხელმისაწვდომი იყოს. Firefox-ის წყაროს კოდი საჯაროდ ხელმისაწვდომია და ამიტომ, შემოქმებას ექვემდებარება - ეს გადამწყვეტი ფუნქციაა პროგრამული უზრუნველყოფის ნდობისა და უსაფრთხოებისთვის.

• Firefox-ს აქვს უამრავი შესაძლებლობა, გააფართოვოს თავისი ფუნქციები დანამატებით (Addons).

• Firefox-ის დაყენების შემდეგ გადადით პარამეტრებში „კონფიდენციალურობის და უსაფრთხოების“ განყოფილებაში, გამორთეთ პაროლების შენახვა (ისინი უნდა იყოს შენახული მხოლოდ თქვენი პაროლის მენეჯერში, როგორც ეს ზემოთ აღვნიშნეთ).

• დააყენეთ „შინაარსის ბლოკირება“ „მკაცრად“.

• ასევე, შეგიძლიათ გამოიყენოთ Brave Browser, რომელიც არის უფასო და ღია კოდზე დაფუძნებული ბრაუზერი, რომლის მთავარი ფოკუსი არის პრივატულობის დაცვა და ავტომატურად ბლოკავს ონლაინ რეკლამებსა და ვებსაიტების ტრეკერებს ნაგულისხმევ პარამეტრებში.

დააინსტალირეთ ბრაუზერის დანამატები

• Firefox-ში გადადით „Addons“ და დააინსტალირეთ შემდეგი დანამატები:

✓ "Ublock Origin" ბლოკავს ყველა რეკლამას. რეკლამა ხშირად შეიცავს არასასურველ კოდს მესამე მხარის ვებსაიტებიდან და შეიძლება ბოროტად იქნას გამოყენებული თქვენს მოწყობილობაზე თავდასხმისთვის.

✓ „HTTPS Everywhere“ დარწმუნდება, რომ თქვენი კავშირები ვებსაიტებთან დაშიფრულია SSL/TLS სერტიფიკატით ყოველთვის, როცა ვებ სერვერიდან ამის მხარდაჭერა აქვს. თუ გსურთ უფრო ძლიერი დაცვა და ბრაუზინგის დროს არ შეწუხდებით, "NoScript" გაძლევთ საშუალებას, დაბლოკოთ ყველა JavaScript კოდი საიტებზე. ეს უზრუნველყოფს ძლიერ დაცვას თავდასხმებისგან, მაგრამ ამან ასევე შეიძლება გამოიწვიოს ზოგიერთი ვებსაიტის არასწორად ჩვენება. წაიკითხეთ NoScript -ის დოკუმენტაცია, რომ ისწავლოთ მისი უკეთ გამოყენება.

✓ „Facebook Container“ გამოყოფს ბრაუზერის ჩანართს, რომელსაც იყენებთ Facebook-ის გასახსნელად ყველა სხვა ვებგვერდისგან. ამ გზით, ის ხელს უშლის Facebook-ს თვალყური ადევნოს სხვა ვებგვერდებს, რომლებიც გახსნილი გაქვთ.

მოემზადეთ მავნე ფიშინგის შეტევებისთვის

• ფიშინგი ციფრული თავდასხმების ერთ-ერთი ყველაზე ფართოდ გამოყენებული და ხშირად წარმატებული ფორმაა, რადგან მომხმარებლები ადვილად ტყუვდებიან ხოლმე.

• ფიშინგი არის ყალბი ელ.ფოსტის ან ვებსაიტების გამოყენება, რომლებიც ძალიან არის ორიგინალს მიმსგავსებული.

• ფიშინგის შეტევების მიზანია მოგატყუოთ, რომ თავდამსხმელი არის ის, ვინც სინამდვილეში არ არის. როგორც კი მის ხრიკს წამოეგებით, თავდამსხმელი ჩვეულებრივ შეეცდება გამოგიგზავნოთ:

(ა) მავნე პროგრამით ინფიცირებული ფაილი,

(ბ) ბმული მავნე ვებსაიტზე, რომელსაც შეუძლია დააინფიციროს თქვენი მოწყობილობა, ან

(გ) ყალბი ვებსაიტის ბმული (როგორიცაა ყალბი Gmail ან ონლაინ ბანკინგის გვერდი), რომელზეც თქვენ უნებლიეთ გაუზიარებთ თქვენს იუზერნეიმს და პაროლს თავდამსხმელს.

• ფიშინგის შეტევებისგან თავის დასაცავად, იყავით უკიდურესად ეჭვიანი ყველა ბმულზე ან დანართ ფაილზე, რომელსაც იღებთ ელექტრონული ფოსტით, WhatsApp-ით, Signal-ით, Facebook-ით, Twitter-ით ან სხვა არხებით.

• გადაამოწმეთ ყველა ბმული, რომელსაც მიიღებთ მასზე დაწკაპუნებამდე. გადაჰყავხართ თუ არა მას ლეგიტიმურ URL / ვებ მისამართზე? არის თუ არა მართლწერის შეცდომები ან მსგავსი, მაგრამ განსხვავებული სიმბოლოები URL-ში? (მაგალითად, www.go.oogle.com-ს არაფერი აქვს საერთო www.google.com-თან, მიუხედავად ძალიან მცირე განსხვავებისა, რომელიც შეიძლება ერთი შეხედვით ვერც შეამჩნიოთ.

• არ ენდოთ ელ.ფოსტის დანართებს, თუ დარწმუნებული არ ხართ, რომ ისინი სანდო პირისგან მოდის. გაფრთხილება: ელ.ფოსტაში გამომგზავნის მისამართი არ ნიშნავს პირადობის დადასტურებას, ის ადვილად შეიძლება გაყალბდეს. თუ ეჭვი შეგეპარათ, დაურეკეთ გამგზავნს და ჰკითხეთ, ნამდვილად გამოგიგზავნათ თუ არა ეს ფაილი.

• ჰკითხეთ საკუთარ თავს: ველოდები რაიმე წერილის მიღებას? ან დანართს თუ ამ ბმულს? თუ ეჭვი შეგეპარათ, დაურეკეთ გამგზავნს და ჰკითხეთ, ნამდვილად გამოგიგზავნათ თუ არა ეს ფაილი. (ვირუსის შემცველი დანართი იყო - ყალბი ელ.წერილით, რომელიც თითქოს გაეროსგან იყო - რომელმაც რუს სახელმწიფო ჰაკერებს წვდომა მისცა გერმანიის პარლამენტის შიდა ქსელზე.)

• ყურადღება მიაქციეთ ენისა და გრაფიკის ხარისხს ელ.ფოსტაში. ხანდახან, ფიშინგური ელ.ფოსტა ცუდი ენითაა დაწერილი ან შექმნილი. თუმცა, სიფრთხილე გვამრთებს: მიზანმიმართული და პროფესიონალური ფიშინგ შეტევა იდეალურად გამოიყურება და შესაძლოა იდეალურად იყოს დაწერილი.

• შეამოწმეთ ელ.ფოსტის სათაური. Gmail-ში გახსენით წერილი და გადადით ელ.ფოსტის თვისებებზე. დააწკაპუნეთ "ორიგინალის ჩვენება". დარწმუნდით, რომ ფოსტის სერვერების დომენის სახელები შეესაბამება გამგზავნის ელ.ფოსტის მისამართს.

• შემდეგი ორი ონლაინ ტესტი საშუალებას გაძლევთ ივარჯიშოთ და გამოცადოთ თქვენი „ფიშინგის დაცვის უნარები”. ისინი მოწოდებულია Google-ის https://phishingquiz.withgoogle.com) და OpenDNS-ის მიერ (https://www.opendns.com/phishing-quiz) უფასოდ.

გამოიყენეთ სანდო VPN სერვისი

• VPN (ვირტუალური პირადი ქსელი) შეიძლება გამოყენებულ იქნას დაშიფრული გვირაბის შესაქმნელად თქვენს მოწყობილობასა და სანდო ორგანიზაციის ან კომპანიის სერვერს შორის. ეს სერვერი შემდეგ გადასცემს თქვენს ტრაფიკს ღია ინტერნეტს.

• ამდენად, VPN იცავს ყველა მონაცემს, რომელსაც თქვენ აგზავნით თქვენი მოწყობილობიდან არასანდო ქსელის მეშვეობით როგორიცაა (ა) საზოგადოებრივი Wi-Fi აეროპორტში, კაფეში ან მატარებლის სადგურზე, ან (ბ) ნებისმიერი ინტერნეტ კავშირი ქვეყნებში, სადაც ხელისუფლება მტრულად განწყობილია და მომხმარებლებს მკაცრად აკონტროლებს.

• ყოველთვის ჩართეთ VPN, როდესაც იყენებთ ერთ-ერთ არასანდო ქსელს.

• ზოგიერთი VPN პროვაიდერი გვთავაზობს საკუთარ აპებს მობილური მოწყობილობებისა და კომპიუტერებისთვის მათ VPN სერვერებთან დასაკავშირებლად. ბაზარზე სხვადასხვა VPN კლიენტის არჩევაა შესაძლებელი.

• ასევე შეგიძლიათ VPN გამოიყენოთ გეობლოკირების გვერდის ასავლელად, რაც ნიშნავს იმას, რომ შეგიძლიათ დაუკავშირდეთ ვებსაიტებსა და ონლაინ სერვისებს, რომლებიც დაბლოკილია თქვენს ლოკაციაზე.

• გახსოვდეთ, რომ VPN არ გაძლევთ სრულ ანონიმურობას. VPN პროვაიდერმა (ანუ კომპანიამ, რომელიც მასპინძლობს თქვენს VPN სერვერს) ყოველთვის იცის, ვინ ხართ და რომელ საიტებს ეწვიეთ ონლაინ. ამიტომ ძალიან მნიშვნელოვანია სანდო პროვაიდერის არჩევა.

• არ გამოიყენოთ უფასო VPN პროვაიდერი — ისინი ჩვეულებრივ ფულს შოულობენ თქვენი მონაცემების გაყიდვით.

გამოიყენეთ Tor ბრაუზერი, როდესაც სრული ანონიმურობა გჭირდებათ

• Tor ბრაუზერი უზრუნველყოფს რეალურ ანონიმურობას ვებ გვერდის დათვალიერებისას. თუ იყენებთ Tor-ს ბრაუზერს, არც ერთ ვებსაიტს, რომელსაც თქვენ სტუმრობთ, არ შეუძლია თქვენი ვინაობის იდენტიფიცირება ან თქვენი მოძრაობების თვალყურის დევნება ქსელის მასშტაბით.

• ძლევამოსილმა დამკვირვებელმაც (სახელმწიფო) კი, რომელსაც შეუძლია მთელ ინტერნეტზე დაკვირვება, არ უნდა შეძლოს თქვენი იდენტობის დადგენა.

• თუ ნამდვილად გჭირდებათ სრული ანონიმურობის შენარჩუნება, აუცილებლად უნდა დაიცვათ შემდეგი წესები:

✓ არ ჩამოტვირთოთ ტორენტები Tor-ზე, რადგან Bittorrent არის ე.წ. peer-to-peer პროტოკოლი, რომელსაც შეუძლია თქვენი IP მისამართის გაგება და თქვენი დე-ანონიმიზაცია.

✓ არ ჩართოთ ან დააინსტალიროთ ბრაუზერის სხვა დანამატები (Addons), გარდა იმისა, რაც წინასწარ დაინსტალირებულია Tor ბრაუზერში. ყველაფერი რაც თქვენ უსაფრთხოებისთვის გჭირდებათ, უკვე ჩაშენებულია.

✓ არ გახსნათ Tor-ის საშუალებით გადმოწერილი დოკუმენტები, როდესაც ონლაინ ხართ. იყავით ძალიან ფრთხილად, როდესაც დოკუმენტების ჩამოტვირთვა Tor-ის საშუალებით ხდება (განსაკუთრებით DOC და PDF ფაილები, თუ არ იყენებთ PDF-ს წამკითხველს, რომელიც ჩაშენებულია Tor ბრაუზერში). ეს დოკუმენტები შეიძლება შეიცავდეს ე.წ „აქტიურ რესურსებს“, რომლებიც ჩამოიტვირთება Tor-ის გარე აპლიკაციის მიერ, რომელიც მათ გასახსნელად გამოიყენება. ეს გამოავლენს თქვენს IP მისამართს და შეუძლია თქვენი ანონიმურობის დარღვევა.

✓ არ გამოიყენოთ Tor ბრაუზერი ვებსაიტებისთვის, რომლებშიც სახელისა და პაროლის შეყვანა მოგიწევთ (როგორიცაა Facebook). მას შემდეგ, რაც ფეისბუქმა იცის ვინ ხარ, მან შეიძლება შენი ანონიმურობა დაარღვიოს ან ვინაობა გაამხილოს.

• გაითვალისწინეთ, რომ Tor ბრაუზერი არ იცავს თქვენი კომპიუტერის მთელ ინტერნეტ ტრაფიკს, როგორიცაა ელფოსტის პროგრამები, ჩეთები ან სხვა ბრაუზერები, ის მხოლოდ გიცავთ იმ საიტების დათვალიერებისას, რომელსაც Tor ბრაუზერის მეშვეობით ეწვევით. მთლიანი ინტერნეტ ტრაფიკის დასაშიფრად გამოიყენეთ VPN კლიენტი.

კომუნიკაციების დაცვა, კონფიდენციალურობა თანამედროვეზე სმარტფონებზე და ადგილობრივად შენახული მონაცემების დაცვა

კომუნიკაციების დაცვა მცირე ჯგუფებში

• კარგი შეტყობინებების აპი არის ღია კოდის პროგრამული უზრუნველყოფა, რომელიც შიფრავს თქვენს შინაარსს ბოლომდე და მაქსიმალურად იცავს თქვენი კომუნიკაციის მეტამონაცემებს.
• პირადი შეტყობინებებისთვის და მცირე ჯგუფებში, ასევე სატელეფონო და ვიდეო ზარებისთვის, გამოიყენეთ Signal ან Wire Messenger. ორივე გთავაზობთ ძლიერ დაშიფვრას ყველა იმ კონტენტისთვის, რომელსაც სხვებთან ცვლით.

• გადაამოწმეთ თქვენი დაშიფვრის გასაღებები საუბრის ყველა მნიშვნელოვან პარტნიორთან. Signal-ში მათ უწოდებენ "უსაფრთხოების ნომერს" და მათი გადამოწმება შესაძლებელია კომუნიკაციის პარტნიორის მოწყობილობაზე QR კოდის სკანირებით. Wire-ში მათ უწოდებენ "თითის ანაბეჭდს", რომელიც შედგება შემთხვევითი რიცხვებისა და ასოების სტრიქონისაგან და საჭიროა მათი ხელით შედარება მოწყობილობებში. ორივეს ნახავთ თითოეული აპლიკაციის შესაბამისი საუბრის პარამეტრებში.
• ჯგუფური სატელეფონო ან ვიდეო ზარებისთვის ასევე შეგიძლიათ გამოიყენოთ უფასო და დაშიფრული ვებ სერვისი Jitsi Meet. Jitsi საშუალებას გაძლევთ, მოიწვიოთ მონაწილეები უბრალოდ მათთან ბმულის გაზიარებით (მაგალითად Signal-ში, Wire-ში ან ელექტრონული ფოსტის საშუალებით). მონაწილეები ხსნიან ბმულს Firefox ან Brave ბრაუზერში და პირდაპირ ემატებიან ჯგუფურ ზარს. ასევე არის Jitsi Meet მობილური აპლიკაცია Android-ისა და iPhone-ის მომხმარებლებისთვის.

თანამშრომლობა და მონაცემთა გაზიარება

Mailbox.org და Nextcloud Collabora Office-თან ერთად გთავაზობთ ბევრ იმავე სერვისს, რაც გააჩნია Microsoft-ს და მომხმარებლებს ჰპირდება ძლიერ კონფიდენციალურობის დაცვას და ჰოსტინგს ევროკავშირის ტერიტორიაზე. Nextcloud უზრუნველყოფს დამატებით შესაძლებლობას, ჰოსტინგი გქონდეთ სახლში ან აირჩიოთ სანდო ჰოსტინგის პროვაიდერი.

გამოიყენეთ მხოლოდ სანდო პროგრამები/აპლიკაციები და შეზღუდეთ მათი ნებართვები

• სმარტფონის აპები ხშირად დიდი რაოდენობის ნებართვებს საჭიროებენ თქვენს ტელეფონზე და აქვთ წვდომა ბევრ პერსონალურ მონაცემზე. მათ შეუძლიათ აკონტროლონ თქვენი აპლიკაციის გამოყენება და ისინი შეიძლება შეიცავდნენ მესამე მხარის ანალიტიკის კოდს.

• ახალი აპის ან პროგრამის ინსტალაციამდე და გამოყენებამდე, დარწმუნდით, რომ იცით რას აკეთებს და საიდან მოდის ის. გახსოვდეთ: ყველა აპლიკაცია ან პროგრამა არის პოტენციური თავდასხმის ვექტორი თქვენს წინააღმდეგ ან შეიძლება შეაგროვოს პერსონალური ინფორმაცია თქვენს შესახებ. გადაამოწმეთ შემდეგი ინფორმაცია:

✓ ვინ ქმნის აპს ან პროგრამას, რომლის გამოყენებაც გსურთ? კომპანია? კერძო პირი? სად არიან ისინი დაფუძნებული?

✓ როგორია აპლიკაციის შემქმნელის ბიზნეს მოდელი? ყიდიან აპს? ან რეკლამა? ან არის აპლიკაციის შემუშავება არაკომერციული ან სხვაგვარად დაფინანსებული?

✓ ღიაა თუ არა აპლიკაციის წყაროს კოდი, რათა დამოუკიდებლად დადასტურდეს, რას აკეთებს პროგრამა? თუ ის აგებულია კომპანიის საკუთრებაში არსებულ დახურულ, საკუთრების წყაროზე?

✓ აპი ან პროგრამა ჯერ კიდევ შენარჩუნებულია? არის თუ არა რეგულარული განახლებები, რომელიც აგვარებს უსაფრთხოების პრობლემებს?

✓ ვენდობი თუ არა აპლიკაციის შემქმნელს საქმეების სწორად შესრულებაში?

• თქვენს სმარტფონზე გადადით ტელეფონის პარამეტრებზე და შეძლებისდაგვარად შეზღუდეთ თითოეული აპლიკაციის ნებართვები.

• რეგულარულად შეამოწმეთ, გაქვთ თუ არა დაინსტალირებული აპები ან პროგრამები, რომლებსაც აღარ იყენებთ. წაშალეთ ის, რაც აღარ გჭირდებათ, რადგან ყველა აპი ან პროგრამა არის პოტენციური თავდასხმის ვექტორი თქვენს წინააღმდეგ ან შეიძლება შეაგროვოს პერსონალური ინფორმაცია თქვენს შესახებ.

ჩაკეტეთ ყველა თქვენი მოწყობილობა

• iPhone-ებზე და თანამედროვე Android სმარტფონებზე (Android ვერსია 8 ან უფრო ახალი) გამოიყენეთ თითის ანაბეჭდი, FaceID ან PIN თქვენი ეკრანის ჩასაკეტად, თუ არ ენდობით სმარტფონის მწარმოებელს თქვენი ბიომეტრიული მონაცემების დამუშავებაში.

• თუ შესაძლებელია, ასევე დაამატეთ ძლიერი პაროლი (იხ. „პაროლები“ ზემოთ), რომელიც მხოლოდ ტელეფონის გადატვირთვისას დაგჭირდებათ.

• გაითვალისწინეთ, რომ თითის ანაბეჭდისა და FaceID-ის მოპარვა უფრო ადვილია, ვიდრე ძლიერი პაროლის. განსაკუთრებით საერთაშორისო საზღვრების გადაკვეთისას, გამორთეთ თქვენი თითის ანაბეჭდი ან FaceID და ამის ნაცვლად გამოიყენეთ ძლიერი პაროლი თქვენი ტელეფონის დასაბლოკად.

• iPhone-ებსა და თანამედროვე Android სმარტფონებზე ლოკალური მეხსიერება ნაგულისხმევად დაშიფრულია. ძველ Android ტელეფონებზე დაშიფვრა ხელით უნდა გააქტიურდეს ტელეფონის პარამეტრებში. თუ დაშიფვრა მიუწვდომელია თქვენი ტელეფონისთვის, უნდა შეიძინოთ სხვა ტელეფონი.

• გააქტიურეთ Screen Lock თქვენს კომპიუტერზე, თუნდაც მცირე ხნით დგებოდეთ მისგან, მაინც დაბლოკეთ ის Win+L მალსახმობით.

• ყოველთვის დააინსტალირეთ განახლებები, როდესაც მას გთავაზობთ თქვენი კომპიუტერი, ტელეფონი ან აპების მაღაზია.

დაშიფრეთ თქვენი კომპიუტერი ადგილობრივად

• მაშინაც კი, თუ თქვენი მონაცემების უმეტესობა ინახება ონლაინ ანგარიშებში, მათი ნაწილი ყოველთვის რჩება თქვენს ადგილობრივ მყარ დისკზე. ამიტომ, მნიშვნელოვანია, დაშიფროთ ყველა თქვენი ადგილობრივი მონაცემებიც.

• Mac კომპიუტერებზე შეგიძლიათ გამოიყენოთ FileVault.

• Windows 10 Professional კომპიუტერებზე Bitlocker. Windows 10-ის სხვა ვერსიებზე, შესაძლოა გქონდეთ შესაძლებლობა, გააქტიუროთ „მოწყობილობის დაშიფვრა“ საკონტროლო პანელში. თუ არა, ამის ნაცვლად დააინსტალირეთ VeraCrypt და გამოიყენეთ იგი მყარი დისკის სრულად დასაშიფრად. VeraCrypt-ს ასევე აქვს შესაძლებლობა შექმნას დაშიფრული კონტეინერის ფაილები, რომლებიც შეიძლება შეივსოს მგრძნობიარე ინფორმაციით. მას ასევე შეუძლია

შექმნას ფარული ფაილების კონტეინერი ან თუნდაც მთელი ფარული ოპერაციული სისტემები. წაიკითხეთ მისი დოკუმენტაცია დამატებითი ინფორმაციისთვის.

• ყველა ზემოაღნიშნული შემთხვევისთვის გამოიყენეთ ძლიერი საპაროლო ფრაზა, რომელსაც ადვილად დაიმახსოვრებთ, რადგან თქვენ მოგიწევთ მისი აკრეფა ყოველ ჯერზე, როცა მოწყობილობას ჩართავთ.

შეამცირეთ თქვენი მონაცემთა კვალი

• ფრთხილად იყავით, რადგან ბევრი აპლიკაცია და პროგრამა ინახავს თქვენ შესახებ ისტორიულ ინფორმაციას და მეტამონაცემებს. ორგანიზაციულ დონეზე, ყველა გუნდი აგროვებს დიდი რაოდენობით მონაცემებს წლების განმავლობაში მათი მუშაობის გზით, როგორიცაა ელ.წერილი, ფაილები, არქივები, დათვალიერების მონაცემები, ჩატის ისტორიები და ა.შ.

• ამ მონაცემების არასწორ ხელში ჩავარდნის თავიდან ასაცილებლად:

✓ ზოგადად: დაიწესეთ წაშლის პოლიტიკა, რომელიც მკაფიოდ განსაზღვრავს, რამდენი ხნით შეინარჩუნოთ გარკვეული ტიპის მონაცემები, სანამ ისინი წაიშლება.

✓ სიგნალში: გააქტიურეთ ფუნქცია „გაქრობადი შეტყობინებები“ თითოეულ საუბარში, განსაკუთრებით უფრო დიდი ჯგუფური ჩეთებისთვის.

✓ Firefox-ში: გამოიყენეთ „მონაცემების გასუფთავება“ და „ისტორიის გასუფთავება“ ფუნქციები რეგულარულად და მექანიკურად (ხელით), რათა მინიმუმამდე დაიყვანოთ წარსული სენსიტიური მონაცემების შენახვა თქვენს მოწყობილობაზე. თქვენ ასევე შეგიძლიათ ამის ავტომატიზაცია, თუ აირჩევთ, ყოველთვის წაშალოთ ასეთი მონაცემები Firefox-ის დახურვისას.

✓ Microsoft Office-ში ან LibreOffice-ში: რეგულარულად გაასუფთავეთ ახლახან გახსნილი ფაილების სია.