4.

ვებ აქტივობის კონტროლი

შენი სმარტფონის ბრაუზერი დიდი რაოდენობის ინფორმაციას ინახავს შენ შესახებ: ადგილმდებარეობა, რას ეძებ ინტერნეტში, რომელ ვებგვერდებს იყენებ - და შეიძლება, ეს ცოდნა მესამე მხარესაც მიაწოდოს.თუმცა რამდენიმე დეტალის ცვლილებით შეგიძლია, ამ ინფორმაციაზე კონტროლი კვლავ მოიპოვო.

ელეფონებში, ტაბლეტებსა და კომპიუტერებში ხშირად ინახება წინასწარ გადმოწერილი ბრაუზერები, რომლებისთვისაც პრიორიტეტული სულაც არაა შენი უსაფრთხოება. მათ ნაცვლად, გირჩევ, გადმოწერო და გამოიყენო ბრაუზერი, რომელიც სპეციალურადაა დაპროგრამებული შენი ვებ აქტივობის დასაცავად ციფრული ტრეკერებისგან.

და კიდევ, შეგიძლია ბრაუზერის დამატებებიც გადმოწერო (ბრაუზერებში მარტივად დასაყენებელი მინიპროგრამები, რომლებიც შენს ონლაინ აქტივობას უფრო დაცულს ხდის).

5.

შენს სოციალური მედიის პოსტებს “ანთეგი” გაუკეთე

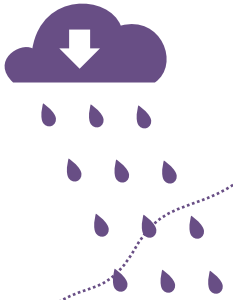
ერთერთი მეთოდი, რომლითაც ციფრულ სერვისებს პერსონალური მონაცემების შეგროვებაში ეხმარები, ფოტოებსა და პოსტებში მეგობრების მონიშვნაა.

შეგიძლია, გასაჯაროებული ინფორმაცია დაიბრუნო (და ამასთანავე სინდისიც შეიმსუბუქო), თუ შენს პოსტებში მეგობრების მონიშვნებს გააუქმებ.

ხმა გაავრცელე! შენს მეგობრებს, ოჯახსა და თანამშრომლებსაც სთხოვე, რომ “გაქცეული” მონაცემების დაბრუნებაში შემოგიერთდნენ. თუ ერთიანი ძალებით ვიმუშავებთ, რომ ციფრული ჩანაწერები შევამციროთ, დეტოქსი უფრო გამარტივდება.

ჯაშუშური რეკლამები და უხილავი ტრეკერები რომ დაბლოკო გადმოწერე uBlock Origin (თავსებადია შემდეგ ბრაუზერებთან: Chrome, Safari და Firefox) ან Privacy Badges (თავსებადია შემდეგ ბრაუზერებთან: Chrome, Safari და Firefox

იმაში დასარწმუნებლად, რომ ვებგვერდებთან შენი კავშირი დაცულია გადმოწერე HTTPS: ბრაუზერის დამატება, რომელიც ვებგვერდებთან კომუნიკაციის დაცულობას უზრუნველყოფს კოდების დაშიფვრით. თუ ბრაუზერად Safari-ს იყენებ, მაგრამ მაინც გსურს ამ სერვისის გააქტიურება, შეგიძლია შენს მთავარ საძიებო სისტემად აირჩიო DuckDuckGo ან ნებისმიერი მსგავსი პროგრამა, რომელიც არ არის Google-ის პროდუქტი. ამ შემთხვევაში შენი კავშირი ავტომატურად გაიშიფრება და დაგიცავს.



DATA DETOX KIT

გააკონტროლე შენი სმარტფონის მონაცემები

რათა თავი დაიცვა ონლაინ სამყაროში

ერთი შეხედვით, შეიძლება სულაც არ მოგეჩვენოს, რომ შენი მონაცემების გასაჯაროება რამე პრობლემას შეგიქმნის: წესით, არც არავის ადარდებს, თუ ქანთრი მუსიკას უსმენ, იმაზე ხშირად ყიდულობ ფეხსაცმელებს, ვიდრე გჭირდება ან შვებულების დაგეგმვას ერთი წლით ადრე იწყებ.

თუმცა პრობლემა ისაა, თუ ვის ხელში აღმოჩნდება ხოლმე ეს ინფორმაცია და რა მიზნით მუშავდება. დროთა განმავლობაში მონაცემები გროვდება და შენზე პირადული ციფრული დეტალების გარკვევა ხდება შესაძლებელი: ჩვევებზე, გადაადგილებაზე, ურთიერთობებზე, აზრებსა და საიდუმლოებზე იგებენ ბიზნესები და მონაცემთა ბროკერები, რომლებიც ამ ინფორმაციას აანალიზებენ და შემდეგ კომერციულ მოგებას იღებენ.

მონაცემთა დეტოქსის ეს ნაწილი საშუალებას მოგცემს, თვალი შეავლო ციფრული ინფორმაციის შეგროვების პრაქტიკას და შესაბამისი ზომებიც მიიღო, რომ საკუთარი თავი დაიცვა ინტერნეტსამყაროში.

მოდი, საქმეს შევუდგეთ!

A product of
TACTICAL TECH

Supported by
Firefox

datadetoxkit.org
#datadetox

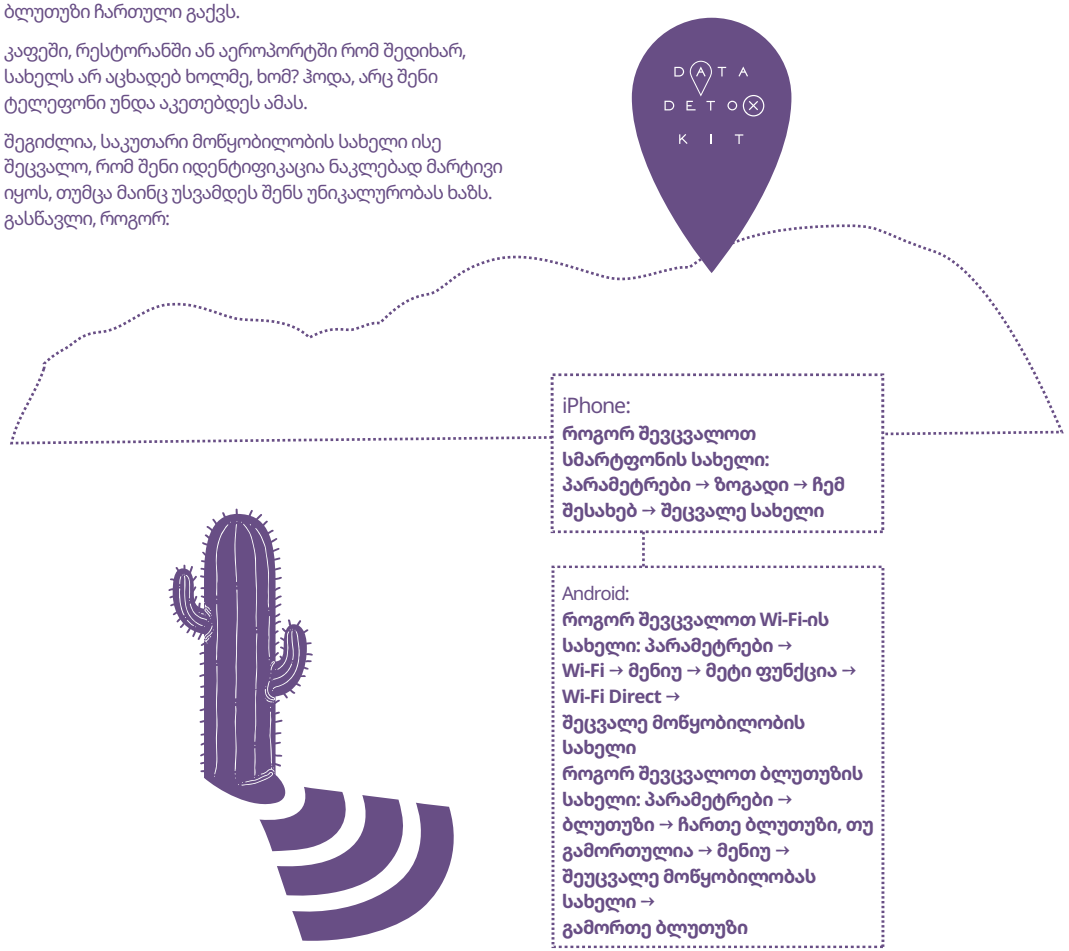
1.

შეცვალე შენი მოწყობილობის სახელი

თავის დროზე, ალბათ შენც "დაარქვი" სახელი ტელეფონს Wi-Fi-ისთვის, ბლუთუზისთვის ან შეიძლება ორივესთვისაც - ან, იქნებ, საერთოდაც ავტომატურად გენერირდა სახელი სისტემის გადმოწერისას. რაც უნდა იყოს, ეს მაინც ნიშნავს, რომ შენი სახელის ნახვა შეუძლიათ როგორც ინტერნეტის პროვაიდერს, ისე შენ გარშემო მყოფ ადამიანებსაც, თუ, რა თქმა უნდა, ბლუთუზი ჩართული გაქვს.

კაფეში, რესტორანში ან აეროპორტში რომ შედიხარ, სახელს არ აცხადებ ხოლმე, ხომ? ჰოდა, არც შენი ტელეფონი უნდა აკეთებდეს ამას.

შეგიძლია, საკუთარი მოწყობილობის სახელი ისე შეცვალო, რომ შენი იდენტიფიკაცია ნაკლებად მარტივი იყოს, თუმცა მაინც უსვამდეს შენს უნიკალურობას ხაზს. გასწავლი, როგორ:



iPhone:
როგორ შევცვალოთ სმარტფონის სახელი: პარამეტრები → ზოგადი → ჩემ შესახებ → შეცვალე სახელი

Android:
როგორ შევცვალოთ Wi-Fi-ის სახელი: პარამეტრები → Wi-Fi → მენიუ → მეტი ფუნქცია → Wi-Fi Direct → შეცვალე მოწყობილობის სახელი
როგორ შევცვალოთ ბლუთუზის სახელი: პარამეტრები → ბლუთუზი → ჩართე ბლუთუზი, თუ გამორთულია → მენიუ → შეუცვალე მოწყობილობას სახელი → გამორთე ბლუთუზი

2.

წაშალე შენი ადგილმდებარეობის ჩანაწერები

რომც მოგეჩვენოს, რომ შენი ადგილმდებარეობა დიდი არაფერი ინფორმაციაა, ეს მონაცემები რომ ერთად იკრიბება, შენ შესახებ ბევრი მნიშვნელოვანი დეტალის გარკვევა ხდება შესაძლებელი: მაგალითად, სად ცხოვრობ, სად მუშაობ და სად გიყვარს ხოლმე მეგობრებთან ერთად გართობა. სწორედ ამიტომ ცდილობენ ხოლმე კომპანიები და მონაცემთა ბროკერები ლოკაციის ჩანაწერების მოპოვებას.

გირჩევ, თითოეული გადმოწერილი აპლიკაციის წვდომის პარამეტრები შეამოწმო და ადგილმდებარეობის სერვისი გამორთო. განსაკუთრებული ყურადღება გაამახვილე იმ აპლიკაციებზე, რომლებსაც სულ არ სჭირდება ლოკაციის პარამეტრები გამართულად ფუნქციონირებისთვის (აი, იმ თამაშს დიდს არაფერს შემატებს ცოდნა, თუ სად ხარ) და იმ აპლიკაციებზეც, რომლებსაც შენ თვითონვე არ გსურს, რომ წვდომა ჰქონდეს ამ სერვისზე:

Android:
პარამეტრები → აპლიკაციების მართვა → ლოკაციაზე წვდომის კონტროლი აპლიკაციებში

iPhone:
პარამეტრები → უსაფრთხოება → ლოკაციის სერვისები → ლოკაციაზე წვდომის კონტროლი აპლიკაციებში

3.

"გაასუფთავე" შენი აპლიკაციები

სოციალური მედიის აპლიკაციებს, თამაშებსა და ამინდის აპლიკაციებს ძალიან აინტერესებთ მონაცემები შენ შესახებ... და შეიძლება, საკმარისზე მეტს აგროვებდნენ კიდეც.

იმ აპლიკაციების წაშლა, რომლებსაც არ იყენებ, ციფრული დეტოქსის ერთ-ერთი მნიშვნელოვანი ნაწილია.

თანაც, სმარტფონის გასუფთავებით, ჯერ ერთი, ძვირფას გიგაბაიტებს დაზოგავ, მეორე - ნაკლები ინტერნეტის გამოყენება დაგჭირდება, დაბოლოს, ტელეფონიც აღარ დაგიჯდება ისე სწრაფად.

Android:
პარამეტრები → აპლიკაციები → მონიშნე აპლიკაცია, რომლის წაშლაც გინდა → წაშლა

iPhone:
დიდხანს დააჭირე რომელიმე აპლიკაციას, სანამ მენიუ გამოჩნდება.

წაშალე აპლიკაცია სიიდან.

დაადასტურე აპლიკაციის წაშლა.

4.

დაიცავი შენი ვირტუალური ძვირფასეულობა

ზუსტად ისე, როგორც შენს ძვირფასეულობებს უვლი ხოლმე სახლში, ყურადღება უნდა მიაქციო იმ ინფორმაციასაც, რომელსაც ვირტუალურ სამყაროში ათავსებ - ფინანსური ჩანაწერები იქნება, პასპორტის დასკანერებული ვერსია თუ მისამართი ან ტელეფონის ნომერი, მაინც საჭიროა, რომ დაფიქრდე, სად ინახება ეს მონაცემები და როგორ შეგიძლია მათი დაცვა.

ლოკალური გასუფთავება პატარ-პატარა ცვლილებების განხორციელების სწრაფი საშუალებაა. დილის ყავის პარალელურად შეგიძლია, შენს მეილში სპეციფიკური ინფორმაცია მოძებნო და წაშალო: *ID-ის დასკანერებული ვერსია, საბანკო დეტალები ან თუნდაც მონაცემები შენი დაზღვევის შესახებ*. თუ ისეთი ინფორმაციაა, როგორიც მოგვიანებით კიდევ დაგჭირდება, გადმოიწერე და დაბეჭდე, სანამ ელფოსტიდან წაშლი.

სიღრმისეული გასუფთავება კი უფრო ეფექტიანია და კარგია, წელიწადში ერთხელ მაინც თუ განახორციელებ. შენი მეილისა და სოციალური ქსელების ინფორმაცია კომპიუტერში გადმოიწერე, შემდეგ კი ონლაინ სივრციდან დააარქივე ან წაშალე და ახალი კონტენტის გაზიარება **"სუფთა ფურცლიდან"** დაიწყე.

რჩევა: უბრალოდ წაშლა არაა საკმარისი - დაასუფთავე ნაგვის ყუთი და დროებითი ფაილებიც!

ოლოს მაინც *შენი გადასაწყვეტია*, შენს არქივებს "ქლაუდზე" გადაიტან თუ გარე მეხსიერების ბარათებზე შეინახავ. რა მეთოდსაც უნდა მიმართო, დარწმუნდი, რომ მნიშვნელოვან ინფორმაციას არ დაკარგავ, ძლიერი პაროლით იცავ და შენთვის მოსახერხებელია.

5.

გაუზიარე

ონლაინ სივრცეს "ქსელი" ტყუილად არ ჰქვია. სხვადასხვა გზით **ყველა ერთმანეთს ვუკავშირდებით** - არა მხოლოდ "მეგობრობის" სტატუსით სოციალურ მედიაში, არამედ ელფოსტის კონტაქტებითა და გაზიარებული ფოტოებითაც. როცა შენს ანგარიშებს იცავ, უფრო ძლიერ პაროლებს იაქტიურებ და მონაცემებს ასუფთავებ, მხოლოდ შენ არ სარგებლობ ამით - ოდნავ უფრო დაცული ხდებიან ის ადამიანებიც, რომლებთანაც რამით ხარ დაკავშირებული.

როცა შენს ელფოსტასა და სოციალური მედიის ანგარიშებს ასუფთავებ, *შენი გარშემო მყოფებიც გაითვალისწინე* - შენი დის საბანკო დეტალები, ოფისის გასაღების კოდი ან შვილის პასპორტი რომ არასწორ ხელში აღმოჩნდეს, ზედმეტი თავის ტკივილი გახდება.

გაუზიარე! ციფრული უსაფრთხოების გაზრდისთვის რამდენიმე ნაბიჯიც საკმარისია. მონაცემთა დეტოქსი გაუზიარე შენს მეგობრებს, ოჯახსა და თანამშრომლებს, რომ მათაც შეძლონ ჩვევების გაუმჯობესება.

DATA DETOX KIT

შეცვალე პარამეტრები

რათა დაიცვა შენი მონაცემები

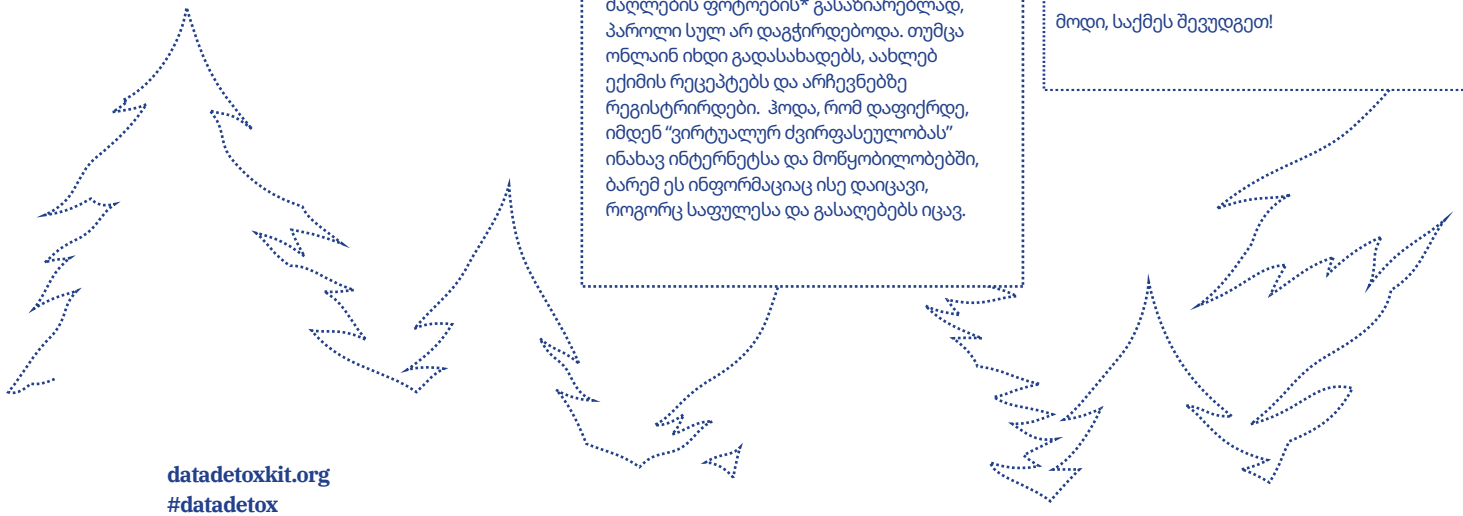
ინტერნეტი რომ მხოლოდ სივრცე იყოს *დინოზავრის კოსტუმში გამოწყობილი ძაღლების ფოტოების* გასაზიარებლად, პაროლი სულ არ დაგჭირდებოდა. თუმცა ონლაინ იხდი გადასახადებს, აახლებ ექიმის რეცეპტებს და არჩევნებზე რეგისტრირდები. ჰოდა, რომ დაფიქრდე, იმდენ "ვირტუალურ ძვირფასეულობას" ინახავ ინტერნეტსა და მოწყობილობებში, ბარემ ეს ინფორმაციაც ისე დაიცავი, როგორც საფულესა და გასაღებებს იცავ.

შენი ვირტუალური ძვირფასეულობების დაცვის ერთი მარტივი ხრიკი **პაროლების გაუმჯობესებაა**. შენს ანგარიშებში შეღწევას არ სჭირდება ბევრი ტექნიკური უნარი - ვარაუდით გამოცნობა ან ავტომატური პროგრამაც საკმარისია.

ერთ ანგარიშს რომ ჩაიგდებენ ხელში, მერე იმავე პაროლს სხვა ქსელებშიც ცდიან, საბოლოოდ კი შენ შესახებ ინფორმაციას შეაგროვებენ, ანგარიშებს წაგართმევენ ან შენი ციფრული იდენტობის განსახიერებას დაიწყებენ.

მონაცემთა დეტოქსი პრაქტიკულ გზებს გასწავლის, თუ როგორ შეგიძლია შენი ონლაინ უსაფრთხოების გაუმჯობესება.

მოდი, საქმეს შევუდგეთ!



A product of
TACTICAL TECH

Supported by
Firefox

datadetoxkit.org
#datadetox

1.

შენი ციფრული კარი ორმაგად ჩარაზე

ეკრანის დაბლოკვა: პაროლით, ფიგურით, თითის თუ სახის ანაბეჭდით, შენი მოწყობილობის დაცვის რამდენიმე საუკეთესო ვარიანტია. თუმცა ასეთი მეთოდი ბევრი არსებობს და შეიძლება, ცოტა გაგიჭირდეს კიდეც შენთვის ყველაზე ხელსაყრელის ამორჩევა.

ტელეფონის, ტაბლეტისა და კომპიუტერის დაბლოკვა უფრო უსაფრთხოა, ვიდრე მუდმივად გახსნილს რომ ტოვებდე. და ზუსტად ისე, როგორც ბევრი ტიპის კარის საკეტი არსებობს, ეკრანის დაბლოკვის ზოგიერთი ვარიანტი დანარჩენებზე უკეთესია.

განსაკუთრებით დაცულია გრძელი, უნიკალური პაროლები ანუ ასოების, ციფრებისა და სიმბოლოების კომბინაცია.

წარმოიდგინე, ეკრანზე თითის გასრიალებით რომ ხსნიდე ტელეფონს. პაროლი რომ გაიაქტიურო, ამით უკვე ერთი ნაბიჯით წინ იქნები დაცულობის საკითხში. ან ფიგურას იყენებ? იქნებ, ეგ ნიმუში გაართულო? შენი პინ კოდი 1234-ია? გირჩევ, კამათელი შვიდჯერ გააგორო და რა ციფრებიც დაგიჯდება, ეგ იყოს შენი ახალი პინი. **ასეთ პატარა ცვლილებებს დიდი შედეგების მოტანა შეუძლია, თუ შენს მოწყობილობაზე კონტროლის მოპოვება გსურს.**

2.

სწორი პაროლი შეარჩიე

“მაგარი” პაროლის შექმნა მარტივია, თუ რამდენიმე პრინციპს გაითვალისწინებ. შენი პაროლი უნდა იყოს:

გრძელი: **პაროლი მინიმუმ რვა ნიშნისგან უნდა შედგებოდეს. 16-20 - კიდევ უკეთესი.**

უნიკალური: **თითოეული ვებგვერდისთვის განსხვავებული პაროლი მოიფიქრე.**

შემთხვევითი: **პაროლი ლოგიკური და მარტივად გამოსაცნობი არ უნდა იყოს. ამაში პაროლ-მენეჯერები დაგეხმარება.**

უძლიერესი პაროლი ასოების, ციფრებისა და სიმბოლოების კომბინაციითაა აგებული. ამ დროში გამოცდილ რჩევას ისევ ვერაფერი ჯობნის რთულად გამოსაცნობი პაროლების შექმნაში. ზოგიერთი სისტემა, სამწუხაროდ, არ გაძლევს სიმბოლოების გამოყენების უფლებას (მაგალითად: @#$%-=+), თუმცა ასოებისა და ციფრების კომბინაცია ხომ მაინც სჯობს მოკლე პაროლს?

იდეალურ შემთხვევაში, შეგიძლია გამოიყენო **პაროლების მენეჯერი**, რომელიც თვითონვე ქმნის და ინახავს შენს კოდებს. სისტემები, მათ შორის 1Password და KeePassXC, რომლებსაც უსაფრთხოების ექსპერტები გვირჩევენ, აპლიკაციებია დანიშნულებით, რომ შენი პირადი ინფორმაცია და სხვა მონაცემები დაიცვან.

3.

გამოიყენე ორი გასაღები

თუ ორმაგი ავთენტიკაცია (2FA) ან რამდენიმეეტაპიანი ავთენტიკაცია (MFA) გაქვს გააქტიურებული, თუნდაც ვინმემ გამოიცნოს შენი პაროლი, მაინც ვერ შეაღწევს შენს მოწყობილობაში ან პროფილზე, თუ ამ დამატებით ფაქტორზე არ აქვს წვდომა.

კიდევ ერთხელ გადაათვალიერე შენ მიერ ყველაზე ხშირად გამოყენებული ვებგვერდებისა და აპლიკაციების უსაფრთხოების პარამეტრები, რომ ორმაგი ავთენტიკაცია შენც გაიაქტიურო. გირჩევ, ყველაზე მნიშვნელოვანი სერვისებით დაიწყო - მაგალითად, ფინანსური აპლიკაციები ან ელფოსტა, რომელიც სხვა ანგარიშებთან გაქვს დაკავშირებული.

Google:
**გახსენი myaccount.google.com →
უსაფრთხოება →
ორმაგი ვერიფიკაცია →
დაიწყე**

Facebook:
**მენიუ →
პარამეტრები →
უსაფრთხოება და სისტემაში შესვლა →
გამოიყენე ორმაგი ავთენტიკაცია**

რჩევა: ვერიფიკაციის კიდევ ერთი ეტაპის დამატების შემდეგ, შენი ვინაობის დამტკიცების ალტერნატიული მეთოდი დაგჭირდება.

4.

ხმა მიაწვდინე

თუ არ მოგწონს ვებგვერდების ჩამთრევი და დამარწმუნებელი დიზაინი ან თუნდაც მისინფორმაცია, შეგიძლია, მეილები დაგზავნო, ტვიტები გამოაქვეყნო და კომპანიებს ხმა მიაწვდინო შენი უკმაყოფილების შესახებ. როცა კომპანიებს მათი ყველაზე ღირებული "აქტივები" - მომხმარებლები აიძულებენ, რომ სხვადასხვა საკითხთან მიდგომა შეცვალონ, უფრო დიდია ალბათობა, რომ მართლაც მოიქცნენ ასე.

თუ მიგაჩნია, რომ შენს უკუკავშირს გამოხმაურება არ მოჰყვება, ერთ ეფექტიან საშუალებას გასწავლი: სხვა ვებგვერდი ან აპლიკაცია გამოიყენე. თუ გარკვეული ონლაინ სერვისით უკმაყოფილებას სიტყვიერად გამოხატავ, ხოლო შემდეგ მის გამოყენებას საერთოდ წყვეტ - საკმარისი რაოდენობის მომხმარებლებიც რომ აგყვნენ, ეს უკვე **აღარ გამორჩება კომპანიას**.

5.

ხმა გაავრცელე

ეს რჩევა მარტივად დასამახსოვრებელი არაა, თუმცა დიდი მასშტაბის შედეგების მოტანა შეუძლია. მეგობრებს, ოჯახის წევრებსა და თანამშრომლებსაც გააგებინე, რამე საეჭვოს თუ შეამჩნევ და სთხოვე, დეტოქსში შემოგიერთდნენ. ციფრული ჩვევების კონტროლი არავისთვისაა მარტივი. თუმცა მნიშვნელოვანია, იპოვო სამოქმედო გზა, რომელიც შენს საჭიროებებსაა მორგებული. ექსპერიმენტებს არ მოერიდო - ხშირ-ხშირად შეცვალე ჩვევები, სანამ საშენო მეთოდს მიაგნებ. არ არსებობს ერთი, კონკრეტული სამოქმედო გეგმა, რომელიც ყველას მოერგება.

დაბოლოს, შენი გადაწყვეტილებები ტექნოლოგიებთან დაკავშირებით გარშემომყოფებსაც გაუზიარე. მაგალითად, თუ აპირებ, რომ საღამოს 8 საათის შემდეგ სასაუბრო აპლიკაციების გამოყენება შეწყვიტო ეკრანთან გატარებული დროის შესამცირებლად, ოჯახის წევრებსა და მეგობრებს სთხოვე, რომ, მოწერის ნაცვლად, დაგირეკონ. დასვი კითხვები, არ მოსწყდე დიალოგს და ონლაინ ცხოვრების დაბალანსებაც არ გაგიჭირდება.

DATA DETOX KIT

თავი დააღწიე "დეფოლტებს"

რათა გაიუმჯობესო შენი ციფრული კეთილდღეობა

გახსენდება, ბოლოს როდის გამოეთიშე ციფრულ სამყაროს და ტექნოლოგია ერთი დღით გვერდით გადადე? მთელი დღით თუ არა, იქნებ ერთი საათით მაინც? თუ გამუდმებით ონლაინ ატარებ ცხოვრებას, მარტო არ ხარ.

მოდი, ჯერ იმას გეტყვი, რომ ტექნოლოგიისკენ დაუძლეველი მიზიდულობა შენი ბრალი სულაც არაა. გინდ დაიჯერე, გინდ - არა – შენი საყვარელი აპლიკაციებისა და ვებგვერდების დიზაინი ისეა ოპტიმიზებული, რომ თითოეულმა დეტალმა, ფერმა თუ ხმამ ჩაგითრიოს და ყოველ ჯერზე მეტი და მეტი მოგანდომოს.

გინდა, იპოვო ოქროს შუალედი ქსელში და ქსელს მიღმა ცხოვრებას შორის? მონაცემთა დეტოქსის ეს ნაწილი ზუსტად ამაში დაგეხმარება.

მოდი, საქმეს შევუდგეთ!

A product of TACTICAL TECH

Supported by Firefox

datadetoxkit.org
#datadetox

1.

რეალობას არ მოსწყდე

ეს რჩევა იმაზე რთულია, ვიდრე ჟღერს და ყოველდღიური ვარჯიში სჭირდება. წარმოიდგინე, კუნთია, რომელსაც მუდმივი წვრთნა სჭირდება, რათა დროთა განმავლობაში გაძლიერდეს. უპირველეს ყოვლისა, გამოიძიე შენი ურთიერთობა ტექნოლოგიებთან.

დღეში რა დროს ატარებ ტელეფონში?

თუ პასუხი არ მოგწონს, არსებობს პარამეტრები და სტრატეგიები, რომელთა დახმარებითაც ისევ მოიპოვებ მოწყობილობებზე კონტროლს.

თუ შენი მიზანია, რომ ფეისბუკზე, ინსტაგრამსა თუ სნეპჩატზე ნაკლები დრო გაატარო, ამ აპლიკაციების პარამეტრები ისე შეცვალე, რომ შენს სურვილებს უკეთ მოერგოს.

ზოგიერთ აპლიკაციას დღიური ლიმიტის შეტყობინებებიც კი აქვს.

Instagram:
პროფილი → მენიუ → პარამეტრები → ანგარიში → შენი აქტივობა → გაიაქტიურე დღიური ლიმიტი

თუ ამჩნევ, რომ შეტყობინებების ზარი თუ ვიბრაცია ადამიანებთან საუბარში ხელს გიშლის, დროებით ხმა გამოურთე, გვერდით გადადე ანდაც ჯიბეში ან ჩანთაში შეინახე, რომ თვალთახედვის არეალიდან მოიშორო.

2.

SPOT THE DESIGN TRICKS

“მუქი ნიმუშები” ინტერფეისის დიზაინის ხრიკია, რომელიც ფსიქოლოგიით აიხსნება და გამოიყენება იმისთვის, რომ რეგისტრაციისკენ, ყიდვისკენ ან ზედმეტი პერსონალური ინფორმაციის გაცემისკენ გიბიძგოს.

ასეთი ხრიკი შეიძლება იყოს გარკვეული ფერი, ღილაკების განლაგება, ბუნდოვანი ტექსტი ან არასრული ინფორმაცია. ზოგიერთი ხრიკი მარტივად აღმოსაჩენია, თუმცა დიდი ნაწილის შემჩნევა მაინც რთულია. ონლაინ შოპინგის ან გამოწერის დროს შეიძლება, შეგიმჩნევია კიდეც ის დეტალები, რომლებიც ჩამოვთვალეთ. დიზაინის მსგავსი ნიმუშები ყველგან არ იქნებოდა, შედეგი რომ არ მოჰქონდეთ - ისინი გვიბიძგებენ, რომ დავაკლიკოთ, გამოვიწეროთ ან უფრო ხშირად ვიყიდოთ რამე პროდუქტი. რაც უფრო მეტი იცი ამ, ერთი შეხედვით, შეუმჩნეველი შეხსენებებისა და მანიპულაციების შესახებ, მით უფრო გამჭრიახი და ინფორმირებული გახდები სხვადასხვა ვებგვერდის გამოყენებისას.

გაგაცნობ რამდენიმე დეტალს, რომლითაც შეძლებ, რომ აპლიკაციების ხრიკებს აჯობო.

შეამჩნიე, როცა გიბიძგებენ: პირველი ნაბიჯი მარტივია - შეიტყვე ამ ხრიკების შესახებ.

“დაასკრინშოტე” და გააზიარე: გადაუღე ეკრანს სურათი და მეგობრებსაც გაუზიარე, როცა ონლაინ რაიმე ხრიკს გადააწყდები (რა თქმა უნდა, პერსონალური დეტალები დამალე - უსაფრთხოება უმთავრესია!). შეგიძლია, კომპანიებსაც სთხოვო, რომ ინტერფეისის დიზაინი შეცვალონ.

სიმშვიდე შეინარჩუნე: თუ ონლაინ მაღაზიაში წამზომს გადააწყდები, დაფიქრდი, ნამდვილად ასეთი საჩქარო თუა რამის ყიდვა. თუ აღმოაჩენ, რომ ღილაკზე შენი სურვილის საწინააღმდეგოდ აკლიკებ, ჯერ ტექსტსა და გამოყენებულ ფერებსაც დააკვირდი. თუ ტექსტის კითხვისას დაიბენი, პირდაპირ არ გადაწყვიტო, რომ შენი ბრალია - შეიძლება, ვებგვერდის ან აპლიკაციის ტერმინოლოგია ბუნდოვანი გამიზნულადაა.

3.

STAY MEDIA SAVVY

თუ შეგიძლია, რომ დიზაინის ხრიკები აღმოაჩინო, შეცდომაში შემყვანი პოსტების შემჩნევასაც მარტივად გაართმევ თავს.

დარწმუნებული ვარ, გსმენია ისეთი ტერმინები, როგორებიცაა “მისინფორმაცია” და “ფეიკ ნიუსი”. თუ დააფიქსირებ, რომ ამბავი განსაკუთრებით გასაკვირია, აღმაშფოთებელია ან ჩვეულებრივზე უფრო კარგად ჟღერს, ჯერ კრიტიკულად დაფიქრდი - მისინფორმაცია არ აღმოჩნდეს.

სანამ ოჯახის წევრებს ან მეგობრებს რამე ამბავს გაუზიარებ, გადაამოწმე.

რომელ ვებგვერდზეა გამოქვეყნებული?
ვინ (და როდის) დაწერა?
სტატიაში რა წერია?
რა წყაროებს ეფუძნება ამბავი?

თუ მისინფორმაციას მიაკვლევ და გსურს, რომ გავრცელებას ხელი შეუშალო, თითქმის ყველა პლატფორმას აქვს პოსტის გასაჩივრების ფუნქცია. შემდეგ კი იმაზეც დაფიქრდი, ღირს თუ არა, რომ მისინფორმაციული სტატიის გამომქვეყნებელი ანგარიში გამოწერილი გქონდეს.

5.

გამოიკვლიე სიმართლე ინტერნეტში

ტერმინი "ფეიკ ნიუსი" მოიაზრებს მცდარ ან შეცდომაში შემყვან ინფორმაციას, მათ შორის, სატირას, არასრულად გამოკვლეულ და გადაუმოწმებელ კონტენტს, სიცრუესა და თაღლითობას. ფეიკ ნიუსს ზოგჯერ ბოროტი განზრახვის გარეშე აზიარებენ ხოლმე, თუმცა, მიზეზის მიუხედავად, შედეგები ერთი და იგივეა: ადამიანები იჯერებენ, რომ მცდარი ინფორმაცია სწორია ან ისეთი რაღაც მოხდა, რაც სინამდვილეში არ მომხდარა.

საუკეთესო შემთხვევაში, ფეიკ ნიუსი შეიძლება სასაცილო მიმი იყოს, უარეს შემთხვევაში კი - ჯანმრთელობის დაცვასთან ან პოლიტიკასთან დაკავშირებული საკითხი.

თუნდაც ძალიან ეცადო, რომ კრიტიკული კითხვები დასვა და ინფორმაცია გამოიკვლიო, შეიძლება მაინც დაგრჩეს ეჭვები. თუმცა გახსოვდეს: მარტო არ ხარ!

6.

დააღწიე თავი ფილტრის ბუშტს

როგორც კი ვებგვერდები და აპლიკაციები შენი ინტერესების პროფილს შექმნიან, ფილტრის ბუშტში აღმოჩნდები, ანუ შენს სიახლეების ველში მხოლოდ ისეთი შინაარსის პოსტები გამოჩნდება, როგორებსაც ხშირად აკლიკებ ხოლმე. რას ნიშნავს ეს ცვლილება შენთვის, როგორც მომხმარებლისთვის?

ფილტრის ბუშტში ყოფნა ნიშნავს, რომ ადამიანები ერთმანეთისგან განსხვავებულ სტატიებს, ახალი ამბების სათაურებსა და რეკლამებს ხედავენ, რაც მარტივად აღსაქმელია ინტერაქციულ სტატიაში "Blue Feed, Red feed" (graphics.wsj.com/blue-feed-red-feed).

თუ იცი, რომ აპლიკაციებსა და ვებპლატფორმებზე ალგორითმულად გენერირებულ კონტენტს ხედავ, რომელიც სპეციალურად შენზეა მორგებული, კითხვა გაგიჩნდებოდა: როგორ შეგიძლია თავი დააღწიო შენს ფილტრის ბუშტს?

DATA DETOX KIT

6 რჩევა, რათა მისინფორმაციის გავლენის ქვეშ არ მოექცე

იმოქმედე

ვებგვერდებმა პასუხისმგებლობა რომც არ აიღონ, არ ნიშნავს, რომ შეცდომებს არ უშვებენ. ყველაზე სანდო პუბლიკაციები სწორედ ისინია, რომლებიც განსაკუთრებულ ყურადღებას აქცევენ სიმართლეს და ჰყავთ თანამშრომლები ან დეპარტამენტები, რომელთა საქმიანობის სფერო ფაქტების გადამოწმებაა.

მიმართულება შეცვალე და ახალი წყაროები მოიძიე

ფილტრის ბუშტისგან თავის დაღწევის ერთი-ერთი კარგი საშუალება სერვისების გამოწერაა, რომლებიც ინფორმაციას სხვადასხვა წყაროდან და პერსპექტივიდან აგროვებენ, შემდეგ კი შეჯამებას აქვეყნებენ. RSS ფიდი და ფორუმები დიდი რაოდენობის მოსაზრებებსა და საკითხებს აგროვებენ, რაც შენი ბუშტის მიღმა არსებული ინფორმაციის აღქმაში დაგეხმარება. ამისთვის კარგი წყაროებია: Global Voices (globalvoices.org) და The Syllabus (the-syllabus.com).

აპლიკაციებს, ვებგვერდებსა და ონლაინ მედიას ახალი ამბების მისაღებად, ხრიკებისა და გართობისთვის ვიყენებთ ხოლმე. თუმცა რთულია, ყურადღება სხვა არასაჭირო რამეზე არ გადაიტანო, როცა რაღაცას ეძებ, ხელმისაწვდომი კონტენტის რაოდენობა კი დღითი დღე იზრდება.

ამასთანავე, ვიდეოში, სურათში ან სტატიაში ფაქტებსა და გამოგონილ ამბებს შორის განსხვავების შემჩნევა არაა ისეთი მარტივი, როგორიც ერთი შეხედვით ჩანს.

რასაც ონლაინ გადააწყდები, ყოველთვის არ შეესაბამება სინამდვილეს - დაწყებული ფსიქოლოგიური ქვიზებით, რომლებიც შენი პიროვნული თვისებების ამოცნობას ცდილობენ, დამთავრებული მანიპულაციური სათაურებით, სურათებითა და ვიდეოებით.

მონაცემთა დეტოქსის ეს ნაწილი დაგეხმარება, მისინფორმაციასთან დაკავშირებული საკითხები გამოიკვლიო - როგორც მარტივი მასალები, ისე შედარებით კომპლექსური, რაც საერთო სურათის აღქმაში დაგეხმარება. ამ ყველაფერთან ერთად კი, რჩევებსაც მიიღებ, თუ როგორ შეგიძლია ეფექტიანად გაიკვლიო გზა ონლაინ სამყაროში.

მოდი, საქმეს შევუდგეთ!

datadetoxkit.org **#datadetox**

A product of TACTICAL TECH

Project partners Save the Children

Funded by the European Union

1.

ინფორმაციული ტალღების შექმნა შენც შეგიძლია

ონლაინ ინტერაქციის ყველაზე გავრცელებული ფორმები პოსტების მოწონება და გაზიარებაა - თითოეულ დაკლიკებას კი დიდი ბიძგების წარმოქმნა შეუძლია. როცა გარკვეული რაოდენობის მომხმარებლები განახორციელებენ ამ ინტერაქციებს, სურათი, ვიდეო თუ პოსტი ისე სწრაფად ვრცელდება, საბოლოოდ "ვირუსული" გახდება ხოლმე.

დაფიქრდი: "რა ზეგავლენა მაქვს ციფრულ სამყაროზე?" ბოლოს როდის გადააწყდი აღმაშფოთებელ ან სასაცილო სტატიას, სათაურს, ვიდეოსა თუ სურათს, რომელიც რამდენიმე წამში უკვე გაზიარებული გქონდა მეგობრებთან? მკვლევრებმა დაადგინეს რომ ვირუსულობის ყველაზე დიდი პოტენციალის მქონე ამბები და სურათები ხშირად მომხმარებლებში შიშს, ზიზღს, სიბრაზესა და შფოთს აღძრავენ. თუ მსგავსი პოსტების გავლენის ქვეშ ხშირად ექცევი, არ იდარდო!

2.

დაფიქრდი, სანამ ფსიქოლოგიურ ქვიზებს შეავსებ

ხომ არ გახსენდება, ბოლოს როდის გადააწყდი ქვიზს (ტექსტურს ან ფილტრს) მსგავსი სათაურით:

> რომელი ათწლეული ხარ?
> რომელი ცხოველი ხარ?
> დისნეის რომელი პერსონაჟი ხარ?
> სად უნდა დაისვენო შემდეგ შვებულებაზე?
> ... სია საკმაოდ გრძელია!

რა თქმა უნდა, ზოგი ქვიზი ნამდვილად იმისთვის იქმნება, რომ სახალისო აქტივობაში ჩაგითრიოს, თუმცა არსებობს შანსიც, რომ თითოეული კითხვა შენს ამოსაცნობად იყოს შექმნილი, ფსიქომეტრიულ პრინციპებზე დაყრდნობით

"სიმპსონების რომელი პერსონაჟი ხარ?" - შენი პასუხები ამ ქვიზისთვის, აპლიკაციებსა და საძიებო სისტემებში გამოვლენილ ციფრულ უნარ-ჩვევებთან ერთად, მონაცემთა ანალიტიკოსებს ეხმარება, შენი ხასიათი და ინტერესები ამოიცნონ, რათა შენი მანიპულაციის უფრო ეფექტიანი გზა დასახონ, მაგალითად, ფეხსაცმლის მოსაყიდად... ან თუნდაც შენი პროფილი შექმნან და გადაწყვიტონ, თუ ზეგავლენის რომელი მეთოდები გიბიძგებს მომდევნო არჩევნებზე გარკვეული გადაწყვეტილებების მისაღებად.

3.

არ წამოეგო ანკესს

ქლიქბეითი ნებისმიერი სენსაციური, თაღლითური ან გამოგონილი სათაურია, რომლის მიზანიც მომხმარებლების პროვოცირებაა, რათა ბმულზე დააკლიკოს. რაც უფრო მეტ გამოხმაურებას მოიპოვებს სტატია, ვიდეო ან სურათი, მით მეტი შემოსავლის გამომუშავებას შეძლებს ავტორიც. შესაბამისად, მანიპულაციური სათაურების შექმნის მოტივაცია საკმაოდ დიდია.

პლატფორმებზე გამოვლენილი ჩვევებით შენი, როგორც მომხმარებლის ციფრული პროფილი ყალიბდება, საბოლოოდ კი სოციალური მედიის კედელზე შენს **ინტერესებსა და ემოციებზე მორგებული სათაურები აღმოჩნდება ხოლმე.

ქლიქბეითი და მისინფორმაცია ხშირად განუყოფელია, თუმცა ყოველთვის - არა. როცა ქლიქბეითების ამოცნობის უნარს გამოიმუშავებ, ყველგან შეამჩნევ - იუთუბზე, ბლოგებსა და ტაბლოიდებზე.

4.

ყურადღება მიაქციე დიფფეიკებს

დიფფეიკი ვიდეო, აუდიო ჩანაწერი ან სურათია, რომელიც ციფრული პროგრამების გამოყენებითაა შექმნილი და ასახავს ადამიანების მანიპულაციურად შეცვლილ გარეგნობას, მოძრაობებსა და საუბარს. "**დიფფეიკი**" შედარებით ახალი ტერმინია, თუმცა პრინციპი უკვე დიდი ხანია არსებობს. უფრო მეტადაა გავრცელებული "იაფფასიანი ფეიკები", რომლის შექმნასაც არ სჭირდება დახვეწილი ტექნოლოგია - მაგალითად, ფოტო ან ვიდეო მცდარი სათაურით და ძველი კონტენტი, რომელიც ახალ ამბებს ერთვის ილუსტრაციად.

ერთი შეხედვით, შეუძლებელი ჩანს დიფფეიკებთან გამკლავება, თუმცა, ყურადღებას თუ არ მოადუნებ, აუცილებლად გამოგივა.

ყურადღება არ მოადუნო და გამოიკვლიე

გადაუმოწმებლად არც ერთ წყაროს არ ენდო - ზუსტად ისე, როგორც ქლიქბეითების ნაწილში ვახსენეთ. თუ რაიმე ვიდეო ან სურათი განსაკუთრებით აღმაშფოთებელი და მიუღებელი ჩანს, ამ ემოციას ყურადღება მიაქციე. ან თუ ერთსა და იმავე სურათს ბევრჯერ გადააწყდი სიახლეების ველში, ესეც საეჭვოა და უმჯობესია, თავდაპირველ წყაროს მიაგნო.

დასვი რამდენიმე კითხვა: ვინ გამოაქვეყნა (რომელმა ვებგვერდმა, ვინ იყო ავტორი)? როდის გამოქვეყნდა? თუ სურათია, სურათის რევერსული ძებნის სისტემა გამოიყენე, როგორიცაა TinEye (tineye.com), რათა წყაროს მიაგნო. ინფორმაცია ახალი ამბების სანდო წყაროებითაც გადაამოწმე, სანამ გადაწყვეტ, რომ ნამდვილია და მეგობრებს ან ოჯახის წევრებს გაუზიარებ.

DATA DETOX KIT

გაზიარება ზრუნვაა

გაზიარება მონაწილეობის ერთერთი ფორმაა. როცა რამეს აზიარებ, ხელს უწყობ მის ვირუსულობასაც. თუ მცდარი ინფორმაცია აღმოჩნდება, გინდა, შენი სახელი და რეპუტაცია მასთან იყოს მიბმული? სანამ ბმულს გააზიარებ, ჯერ დაფიქრდი, მცდარი, მავნებელი ან ტოქსიკური არ იყოს.

ზოგი დეტალი საიდუმლოდ შეინახე

როცა პირად ინფორმაციაზე დაფიქრდები, პირველი, ალბათ, პაროლები, საიდენტიფიკაციო კოდები და საბანკო ანგარიშის ნომრები გაგახსენდება. თუმცა ასევე პირადულია სხვა დეტალებიც, მათ შორის, ის, თუ რა გაშინებს, რა გაღიზიანებს და რა ამბიციები გაქვს. მონაცემთა ანალიტიკოსები ამ წვრილმანებით ხვდებიან, თუ რა გიბიძგებს გარკვეული გადაწყვეტილებებისკენ. ამიტომაც, სანამ ასეთ ინფორმაციას კითხვარში ან ქვიზში გააზიარებ, ჯერ დაფიქრდი.

წყაროები გადაამოწმე

როცა ქლიქბეითს გადააწყდები, მხოლოდ სათაურის შეფასებით არ შემოიფაგლო. თუ ბმული უსაფრთხოა, სტატიას დააკლიკე და გადაამოწმე ავტორი, გამოქვეყნების თარიღი და გამოყენებული წყაროები. შეიძლება სტატიაში ნახსენებიც კი იყოს, რომ დასპონსორებული კონტენტი ან რეკლამაა, ან საერთოდაც - ავტორის მოსაზრება. ეს დეტალები დაგეხმარება, გაარკვიო, ღირს თუ არა, რომ შენი ენერგია დახარჯო ქლიქბეით კონტენტზე.