NDI
NATIONAL DEMOCRATIC INSTITUTE

კიბერუსაფრთხოების სახელმძღვანელო

სთვის

სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის

სახელმძღვანელო სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის, რომლებსაც განზრახული აქვთ შეიმუშაონ კიბერუსაფრთხოების გეგმა



NDI
NATIONAL DEMOCRATIC INSTITUTE

კიბერუსაფრთხოების სახელმძღვანელო

სთვის

სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის

სახელმძღვანელო სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის, რომლებსაც განზრახული აქვთ შეიმუშაონ კიბერუსაფრთხოების გეგმა

მოცემული ნამუშევარი ლიცენზირებულია Creative Commons Attribution-ShareAlike 4.0 საერთაშორისო ლიცენზიით. აღნიშნული ლიცენზიის ასლი იხ. ბმულზე http://creativecommons.org/licenses/by-sa/4.0/ ან მიმართეთ წერილით Creative Commons-ს, PO Box 1866, Mountain View, CA 94042, USA.



შინაარსი

ვიზუალური ნიშნები 4

ტოპ 10 6

ავტორები და მადლიერება 7

ვინ ვართ? 7

ვისთვისაა გამიზნული წინამდებარე „სახელმძღვანელო“? 8

რა არის უსაფრთხოების გეგმა და რატომ უნდა ჰქონდეს ის ჩემს ორგანიზაციას? 8

რა აქტივები გააჩნია თქვენს ორგანიზაციას და რა გსურთ, დაიცვათ? 9

ვინ არიან თქვენი კონკურენტები და რა შესაძლებლობები და მოტივაცია გააჩნია მათ? 9

რა საფრთხეები ემუქრება თქვენს ორგანიზაციას? და რამდენად რეალური და გავლენიანია ისინი? 10

თქვენი ორგანიზაციის კიბერუსაფრთხოების გეგმის შემუშავება 11

უსაფრთხოების კულტურის დანერგვა 12

მოახდინეთ უსაფრთხოების ინტეგრაცია თქვენს ყოველდღიურ საწარმოო სტრუქტურაში 13

მიიღეთ ორგანიზაციული თანხმობა 14

შეიმუშავეთ ტრენინგის გეგმა 14

მყარი საფუძველი: ანგარიშები და მოწყობილობების დაცვა 16

დოკუმენტაციის დაცულობა: პაროლები და აუთენტურობის ორფაქტორული შემოწმება 18

მოწყობილობების დაცვა 26

ფიშინგი: საყოველთაო საფრთხე მოწყობილობების და პროფილებისათვის 32

უსაფრთხო კომუნიკაცია და მონაცემების შენახვა 37

კომუნიკაცია და მონაცემების გაზიარება 38

მონაცემების უსაფრთხოდ შენახვა 50

უსაფრთხოების დაცვა ინტერნეტში 53

უსაფრთხო ბრაუზინგი 54

სოციალური მედიის უსაფრთხოება 64

თქვენი ვებგვერდი ონლაინ რეჟიმში 66

დაიცავით თქვენი WiFi ქსელი 67

ფიზიკური უსაფრთხოების დაცვა 68

ფიზიკური აქტივების დაცვა 70

როგორ იქცევით, როცა საქმე ცუდადაა 74

დანართი „ა“: რეკომენდებული რესურსები 78

დანართი „ბ“: უსაფრთხოების გეგმის საწყისი კომპლექტი 79

ვიზუალური ნიშნები

გარდა ძირითადი ტექსტისა, სახელმძღვანელოში პერიოდულად შეგხვდებათ რამდენიმე ფონზე მოცემული სხვადასხვა ელემენტი. ქვემოთ მოცემული მოკლე „აღწერა“ დაგეხმარებათ ძირითადი ელემენტების გაგებაში:



სიტუაციური ანალიზი

აღნიშნავს თემატურ კვლევებს, რომლებიც ხაზს უსვამს კონკრეტული საკითხის რეალურ გავლენას სამოქალაქო საზოგადოებრივ ორგანიზაციებზე გლობალურად ან კონკრეტულ ქვეყანაში.



დამატებითი რჩევები

აღნიშნავს რამდენიმე დამატებით რეკომენდაციას და ინფორმაციას, რომელსაც ყურადღება უნდა მიაქციოთ „სახელმძღვანელოს“ კითხვისას.



რეალური სამყარო

წარმოადგენს კიბერუსაფრთხოების ტაქტიკების როგორც კეთილი, ისე ბოროტი განზრახვით „რეალურ სამყაროში“ გამოყენებული რესურსების ტიპურ მაგალითებს.



ღრმად

აღნიშნავს გაღრმავებულ საკითხს - ინფორმაციას, რომელიც მნიშვნელოვანია თქვენი ორგანიზაციის მიერ გასათვალისწინებლად, თუმცა, შესაძლოა იყოს მცირედ უფრო ტექნიკური ან რთული.



უსაფრთხოების გეგმის შემადგენელი ბლოკები

აღნიშნავს „უსაფრთხოების გეგმის შემადგენელ ბლოკებს“, რომლებიც წარმოადგენს „სახელმძღვანელოს“ თითოეული სექციიდან ასაღებ საკვანძო დასკვნებს.

1



უსაფრთხოების კულტურის დანერგვა

2



მყარი საფუძველი: პროფილების და მოწყობილობების დაცვა

3



უსაფრთხო კომუნიკაცია და მონაცემების შენახვა

4



უსაფრთხოების დაცვა ინტერნეტში

5



ფიზიკური უსაფრთხოების დაცვა

6



როგორ იქცევით, როცა საქმე ცუდადაა

ტოპ 10

აღნიშნული ათი ელემენტი გადამწყვეტი მნიშვნელობისაა თქვენი ორგანიზაციის უსაფრთხოების გეგმისათვის. თუ გსურთ საიდანმე დაწყება, ჯერ დაიწყეთ აქედან.

1

რეგულარულად ჩაატარეთ ტრენინგი უსაფრთხოების საკითხებზე თქვენს ორგანიზაციაში

2

მზად იყავით ფიშინგისათვის და აწარმოეთ ანგარიშგების სისტემა

3

თუ შესაძლებელია, გამოიყენეთ დაშიფვრა მთელი კომუნიკაციისათვის - თავიდან ბოლომდე

4

მოითხოვეთ საიმედო პაროლები და დანერგეთ პაროლების მენეჯერი მთელს თქვენს ორგანიზაციაში

5

თუ შესაძლებელია, მოითხოვეთ აუთენტურობის ორფაქტორული შემოწმება

6

უზრუნველყავით მთელი პერსონალის მოწყობილობებისა და პროგრამული უზრუნველყოფის დროული განახლება

7

გამოიყენეთ დაცული დისტანციური საცავი მონაცემთა შესანახად

8

გამოიყენეთ HTTP-ები და, საჭიროებისამებრ, VPN-ი ინტერნეტზე წვდომისათვის

9

დაიცავით თქვენი ორგანიზაციის ფიზიკური აქტივები

10

შეიმუშავეთ განსაკუთრებულ შემთხვევებზე რეაგირების ორგანიზაციული გეგმა

ავტორები და მადლიერება

წამყვანი ავტორი: **Evan Summers (NDI)**
თანაავტორები: **Sarah Moulton (NDI); Chris Doten (NDI)**

წინამდებარე „სახელმძღვანელოს“ შემუშავებაში გაწეული დახმარებისათვის გვსურს მადლობა გადავუხადოთ ჩვენს ექსპერტ დამოუკიდებელ რედაქტორებს, რომლებიც, მჭიდრო თანამშრომლობის ფარგლებში, გვაწვდიდნენ მნიშვნელოვან კომენტარებს, კორექტურებს და წინადადებებს, მათ შორის:

Fiona Krakenburger, Open Technology Fund; Bill Budington and Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI-ი; Aaron Azelton, NDI-ი; და Whitney Pfeiffer, NDI.

ასევე გვსურს, აღვნიშნოთ ორგანიზაციული უსაფრთხოების საზოგადოების (OrgSec) მიერ შედგენილი ყველა შესანიშნავი სახელმძღვანელო, ცნობარი, დამხმარე სახელმძღვანელო, ტრენინგის მოდული და სხვა მასალა. წინამდებარე „სახელმძღვანელოს“ მიზანია შეკრიბოს სიღრმისეული მასალები, ერთად შეკრას მთელი გამოცდილება და აქციოს ის ადვილად აღსაქმელ რესურსად სამოქალაქო საზოგადოებრივ ორგანიზაციებისათვის, რომლებსაც განზრახული აქვთ, შეიმუშაონ კიბერუსაფრთხოების გეგმა.

გარდა საზოგადოების მიერ შედგენილი არაერთი შესანიშნავი რესურსით ირიბი ინსპირაციისა, ჩვენ ასევე პირდაპირ გადმოვიტანეთ სასარგებლო ტერმინოლოგია წინამდებარე „სახელმძღვანელოში“ მრავალი არსებული რესურსიდან, კერძოდ, **Electronic Frontier Foundation-ის** „თვალთვალისაგან თავდაცვის სახელმძღვანელოდან“, **Tactical Tech-ის** „ყოვლისმომცველი უსაფრთხოების სახელმძღვანელოდან“ და **Center for Democracy and Technology-ის** და **Freedom of the Press Foundation-ის** მთელი რიგი განმარტებითი ბლოკებიდან. ქვემოთ მოცემულ სექციებში მრავლად შეხვდებით ხსენებული რესურსების სპეციფიურ ციტირებებს, ხოლო **დანართში „ა“** მოცემულია სრულ ბმულები, ავტორი და სალიცენზიო ინფორმაცია.

ასევე დაბეჯითებით გირჩევთ, რომ წინამდებარე „სახელმძღვანელოს“ ნებისმიერმა მკითხველმა ისარგებლოს Open Technology Fund-ის მიერ კომპილირებული და განახლებული ციფრული უსაფრთხოების სახელმძღვანელოების და რესურსების ვრცელი **ბიბლიოთეკით**.

ვინ ვართ?

National Democratic Institute for International Affairs (NDI) არის ვაშინგტონში, კოლუმბიის ოლქში მდებარე არაკომერციული არაპარტიული ორგანიზაცია, რომელიც მუშაობს და თანამშრომლობს მთელს მსოფლიოში დემოკრატიული ინსტიტუციების, პროცესების, ნორმების და ღირებულებების გასაძლიერებლად და დასაცავად ყველა ადამიანისათვის ცხოვრების უკეთესი ხარისხის უზრუნველყოფის მიზნით.

NDI მიიჩნევს, რომ ყველა ადამიანს აქვს უფლება იცხოვროს სამყაროში, სადაც დაცულია მისი ღირსება, უსაფრთხოება და პოლიტიკური უფლებები — და რომ ციფრული სამყარო არ წარმოადგენს გამონაკლისს.

NDI-ს დემოკრატიის და ტექნოლოგიების გუნდის მიზანია ხელი შეუწყოს გლობალურ ციფრულ ეკოსისტემას, რომელშიც დაცული, აღზევებული და გაღვივებული იქნება დემოკრატიული ღირებულებები, მთავრობები იქნება უფრო გამჭვირვალე და ინკლუზიური, ხოლო ყველა მოქალაქეს შეეძლება ჰყავდეს ანგარიშვალდებული მთავრობა. ამ საქმეს ვაკეთებთ კიბერუსაფრთხოების მოქნილი სტრატეგიის აქტივისტების გლობალური ქსელის მხარდაჭერით და წინამდებარე „სახელმძღვანელოს“ მსგავს რესურსებზე მომუშავე პარტნიორებთან თანამშრომლობით. დამატებითი ინფორმაცია ჩვენი საქმიანობის შესახებ შეგიძლიათ, მიიღოთ ჩვენს **ვებგვერდზე**, **Twitter-ზე** ჩვენი გამოყოლით ან მომართვით უშუალოდ **cyberhandbook@ndi.org**. ჩვენ მუდამ მოხარულნი ვართ, მივიღოთ თქვენი გამოხმაურება და ვუპასუხოთ კითხვებს ჩვენს გუნდსა და ჩვენს საქმიანობაზე კიბერუსაფრთხოებასთან, ტექნოლოგიებთან და დემოკრატასთან დაკავშირებით.

ვისთვისაა გამიზნული წინამდებარე „სახელმძღვანელო“?

წინამდებარე „სახელმძღვანელო“ დაიწერა მარტივი მიზნით: დახმარებოდა თქვენს სამოქალაქო საზოგადოებრივ ორგანიზაციას კიბერუსაფრთხოების გასაგები და რეალიზებადი გეგმის შემუშავებაში.

რამდენადაც მსოფლიო უფრო და უფრო მეტად გადადის ონლაინ-რეჟიმში კიბერუსფრთხოება აღარაა მხოლოდ მოდური ტერმინი, არამედ წარმოადგენს გადამწყვეტ კონცეფციას ორგანიზაციის წარმატებისა და მისი გუნდის უსაფრთხოებისათვის. კერძოდ, სამოქალაქო საზოგადოებრივ ორგანიზაციებისათვის, დემოკრატიის, ინტერესების დაცვის, ანგარიშვალდებულების და ადამიანის უფლებების სფეროებში, ინფორმაციის (როგორც ონლაინ, ისე პირიქით) უსაფრთხოება იქცა გამოწვევად, რომელიც ყურადღებას, ინვესტიციას და სიფხიზლეს საჭიროებს.

სავარაუდოდ, თქვენი ორგანიზაცია შეიქნება - თუ უკვე არ შეიქნა – კიბერუსაფრთხოებაზე შეტევის სამიზნე. ეს არ არის პანიკის დათესვის საფუძველი ეს რეალობაა იმ ორგანიზაციებისათვისაც კი, რომლებიც არ მიიჩნევს თავს კონკრეტულ სამიზნედ.

Center for Strategic and International Studies, რომელიც აწარმოებს განახლებად სიას და რომელსაც ისინი "მნიშვნელოვან კიბერ-ინციდენტებს" უწოდებენ, წლიურად, საშუალოდ, აღრიცხავს ასობით სერიოზულ კიბერ-შეტევას, რომელთაგან მრავალი მიზნად ისახავს ერთბაშად, ასეულობით თუ არა, ათეულობით ორგანიზაციას მაინც. გარდა ხსენებული აღრიცხული შეტევებისა, ყოველწლიურად, სავარაუდოდ, ადგილი აქვს ასობით მცირე შეტევას, რომლებიც არ აღირიცხება ან ეცნობება და მრავალი მიზნად ისახავს სამოქალაქო საზოგადოებრივ ორგანიზაციებს, რომლებიც მუშაობს დემოკრატიის, ანგარიშვალდებულების და ადამიანის უფლებების მხარდასაჭერად. ხშირად სამიზნეს წარმოადგენს ქალების ან სხვა მარგინალიზებული ჯგუფების წარმომადგენელი ორგანიზაციები.

აღნიშნულის მსგავს კიბერ-შეტევებს გააჩნია მნიშვნელოვანი შედეგები. მიუხედავად იმისა, არის თუ არა მათი მიზანი თქვენი ფულის დაუფლება, თქვენი ხმის ჩახშობა, თქვენი ორგანიზაციის საქმიანობის შეფერხება, თქვენი რეპუტაციის დაზიანება ან თუნდაც ინფორმაციის მოპარვა, რამაც შესაძლოა გამოიწვიოს თქვენი პარტნიორების თუ პერსონალის ფსიქოლოგიური ან ფიზიკური დაზიანება, აუცილებელია ხსენებული საფრთხეების სერიოზულად აღქმა. კარგი ისაა, რომ თქვენი და თქვენი ორგანიზაციის საყოველთაო საფრთხეებისაგან დასაცავად არაა საჭირო იქცეთ პროგრამისტად ან ტექნოლოგად. თუმცა, მყარი ორგანიზაციული უსაფრთხოების გეგმის შემუშავების და რეალიზაციისას მზად უნდა იყოთ ძალისხმევის, ენერგიის და დროის ინვესტიციისთვის. თუ არასდროს გიფიქრიათ კიბერუსაფრთხოებაზე თქვენს ორგანიზაციაში ან არ გქონდათ დრო მისთვის ყურადღების დასათმობად თუ საკითხის ზოგიერთი საფუძვლის შესასწავლად, მაგრამ ფიქრობთ, რომ თქვენს ორგანიზაციას შეუძლია კიბერუსაფრთხოების დონის ამაღლება, წინამდებარე „სახელმძღვანელო“ თქვენთვისაა. მიუხედავად საფუძვლისა, წინამდებარე „სახელმძღვანელოს“ მიზანია მიაწოდოს თქვენს ორგანიზაციას უსაფრთხოების მყარი გეგმის გასამართად მისთვის აუცილებელი მნიშვნელოვანი ინფორმაცია. გეგმა, რომელიც არ არის უბრალოდ სიტყვების ქაღალდზე დაწერა და გაძლევთ საშუალებას, რეალურად აამუშაოთ აღიარებული მეთოდიკა.

რა არის უსაფრთხოების გეგმა და რატომ უნდა ჰქონდეს ის ჩემს ორგანიზაციას?

უსაფრთხოების გეგმა წარმოადგენს იმ წერილობითი პოლიტიკების, პროცედურების და მითითებების კრებულს, რომლებზეც შეთანხმდა თქვენი ორგანიზაცია უსაფრთხოების იმ დონის მისაღწევად, რომელიც თქვენ და თქვენს გუნდს მიაჩნია შესაფერისად თქვენი ხალხის, პარტნიორების და ინფორმაციის უსაფრთხოებისათვის.

კარგად შედგენილი და განახლებული ორგანიზაციული უსაფრთხოების გეგმა უზრუნველყოფს თქვენს უსაფრთხოებას და ეფექტურობის ამაღლებას თქვენს გონებაში სიმშვიდის დამყარებით, რაც აუცილებელია თქვენი ორგანიზაციის მნიშვნელოვან ყოველდღიურ საქმიანობაზე კონცენტრაციისათვის. ამომწურავი გეგმის გარეშე ფიქრის პროცესში, მეტად მარტივია ვერ ხედავდეთ ზოგიერთი ტიპის საფრთხეს და ზედმეტი ყურადღება დაუთმოთ ერთ რისკს ან არ მიაქციოთ ყურადღება კიბერუსაფრთხოებას მანამ, სანამ არ დადგება კრიზისი. უსაფრთხოების გეგმის შემუშავების დაწყებისას საკუთარ თავს უნდა დაუსვათ რამდენიმე მნიშვნელოვანი კითხვა, რასაც **რისკების შეფასება** ეწოდება. ხსენებულ კითხვებზე პასუხის გაცემა დაეხმარება თქვენს ორგანიზაციას, აღიქვას თქვენს წინაშე არსებული უნიკალური საფრთხეები და საშუალებას მოგცემთ შეჩერდეთ და ყოველმხრივ დაფიქრდეთ, თუ რა გჭირდებათ დაცვისათვის და ვისგან საჭიროებთ დაცვას. ტრენირებულ შემფასებლებს, სტრუქტურის შემმოწმებელი „ინტერნიუსის“ SAFETAG-ის მსგავსი სისტემების გამოყენებით, გააჩნიათ უნარი, დაეხმარონ თქვენს ორგანიზაციას ხსენებული პროცესის გავლაში. თუ შეგიძლიათ მიიღოთ წვდომა ამ დონის პროფესიულ ექსპერტებზე, ეს მართლაც ღირს, მაგრამ სრული შეფასების გარეშეც უნდა შეხვდეთ თქვენს ორგანიზაციას, რათა ღრმააზროვნად განიხილოთ შემდეგი საკვანძო კითხვები:

1 რა აქტივები გააჩნია თქვენს ორგანიზაციას და რა ?

შეგიძლიათ დაიწყოთ ამ კითხვებზე პასუხის გაცემა **თქვენი ორგანიზაციის ყველა აქტივის კატალოგის შექმნით**. ინფორმაცია, როგორიცაა შეტყობინებები, ელ-ფოსტა, კონტაქტები, დოკუმენტები, კალენდრები და ლოკაციები, ყველა წარმოადგენს შესაძლო აქტივს. აქტივი, შესაძლოა, იყოს ტელეფონები, კომპიუტერები და სხვა მოწყობილობები. ასევე, შესაძლოა, აქტივი იყოს ადამიანები, კავშირები და ურთიერთობებიც. შეადგინეთ **თქვენი აქტივების სია** და სცადეთ, მოახდინოთ მათი კატალოგიზება ორგანიზაციისათვის მნიშვნელობის მიხედვით, სადაც შეინახავთ მათ (სავარაუდოდ, რამდენიმე ციფრულ ან ფიზიკურ ადგილზე), ეს კი საშუალებას არ მისცემს სხვებს, იქონიონ მათზე წვდომა და დააზიანონ ან აურიონ ისინი. გახსოვდეთ, რომ ყველაფერი თანაბრად მნიშვნელოვანი არაა. თუ ორგანიზაციის ზოგიერთი მონაცემი საჯაროა ან წარმოადგენს თქვენ მიერ უკვე გამოქვეყნებულ ინფორმაციას, ის არაა საიდუმლო, რომლის დაცვაც გესაჭიროებათ.

2 ვინ არიან თქვენი კონკურენტები და რა შესაძლებლობები და მოტივაცია გააჩნიათ მათ?

„მეტოქე“ არის ტერმინი, რომელიც საყოველთაოდ გამოიყენება ორგანიზაციულ უსაფრთხოებაში. მარტივად რომ ვთქვათ, მეტოქეები არიან ის მოქმედი პირები (ფიზიკური პირები ან ჯგუფები), რომლებიც დაინტერესებული არიან თქვენს ორგანიზაციაზე შეტევით, თქვენი სამუშაოს შეფერხებით და თქვენს ინფორმაციაზე წვდომით, ან მისი განადგურებით: ცუდი ბიჭები. პოტენციური მეტოქეების მაგალითები, შესაძლოა, მოიცავდეს ფინანსურ თაღლითებს, კონკურენტებს, ადგილობრივი თუ ეროვნული დონის უწყებებს თუ მთავრობებს ან იდეოლოგიურად თუ პოლიტიკურად მოტივირებულ ჰაკერებს. მნიშვნელოვანია, შეადგინოთ თქვენი მეტოქეების სია და კრიტიკულად შეაფასოთ ვის შეიძლება სურდეს თქვენს ორგანიზაციაზე და პერსონალზე ნეგატიური გავლენის მოხდენა. გარე მოქმედი პირების (მაგალითად, უცხოური მთავრობა ან კონკრეტული პოლიტიკური ჯგუფი) მეტოქეებად წარმოდგენა მარტივია, მაგრამ ასევე გახსოვდეთ, რომ მეტოქე შეიძლება იყოს თქვენი ნაცნობიც, როგორიცაა უკმაყოფილო თანამშრომელი, პერსონალის ყოფილი წევრი და გაუტანელი ოჯახის წევრი ან პარტნიორი. სხვადასხვა მეტოქე სხვადასხვა საფრთხეს ქმნის და სხვადასხვა რესურსი და შესაძლებლობა აქვს თქვენი საქმიანობის შესაფერხებლად და თქვენს ინფორმაციაზე წვდომის მოსაპოვებლად ან მის გასანადგურებლად.

მაგალითად, მთავრობებს ხშირად ბევრი ფული და მძლავრი შესაძლებლობები აქვთ ინტერნეტის გამორთვის თუ ძვირადღირებული სათვალთვალო ტექნოლოგიების ჩათვლით; მობილურ ქსელებს და ინტერნეტ-პროვაიდერებს, სავარაუდოდ, გააჩნიათ წვდომა ზარების ჩანაწერებზე და ბრაუზინგის ისტორიებზე; კვალიფიციურ ჰაკერებს შეუძლიათ ჩაერთონ საჯარო Wi-Fi ქსელებში სუსტად დაცულ კომუნიკაციებში ან ფინანსურ ტრანზაქციებში. შესაძლოა თქვენს საკუთარ მეტოქედაც კი იქცეთ, მაგალითად, მნიშვნელოვანი ფაილების შემთხვევითი წაშლით ან პირადი შეტყობინებების არადანიშნულებისამებრ გაგზავნით.

მეტოქეების მოტივები, სავარაუდოდ, განსხვავდება მათი შესაძლებლობის, ინტერესების და სტრატეგიის მიხედვით. არიან ისინი დაინტერესებული თქვენი ორგანიზაციის დისკრედიტაციით? იქნებ მათი განზრახვაა, ჩაახშონ თქვენი შეტყობინებები? ან იქნებ ისინი განიხილავენ თქვენს ორგანიზაციას კონკურენტად და სურთ მოიპოვონ უპირატესობა? მნიშვნელოვანია, გავიგოთ მეტოქის მოტივაცია, რადგან ეს შეიძლება დაეხმაროს თქვენს ორგანიზაციას, უკეთ შეაფასოს საფრთხეები, რომლებიც მან შეიძლება წარმოქმნას.

3 რა საფრთხეები ემუქრება თქვენს ორგანიზაციას? და რამდენად რეალური და გავლენიანია ისინი?

შესაძლო საფრთხეების იდენტიფიკაციის შემდეგ, სავარაუდოდ, გექნებათ გრძელი სია, რომელიც შესაძლოა გადაჭარბებული აღმოჩნდეს. შესაძლოა, იგრძნოთ, რომ ნებისმიერი ძალისხმევა უსაგნოა ან არ იცოდეთ, საიდან დაიწყოთ. თქვენი ორგანიზაციის მიერ შემდგომი პროდუქტიული ნაბიჯების გადასადგმელად ძალების მოკრებაში დახმარების მიზნით სასარგებლოა აწარმოოთ თითოეული საფრთხის ანალიზი გამომდინარე ორი ფაქტორიდან: ალბათობა, რომ საფრთხე წარმოიშობა და მისი გავლენა წარმოშობის შემთხვევაში.

საფრთხის ალბათობის გასაზომად (სავარაუდოდ „დაბალი, საშუალო ან მაღალი“ იმისდა მიხედვით, რომ მოცემული შემთხვევა ნაკლებად სავარაუდოა, მოხდეს, შესაძლოა, მოხდეს ან ხდება ხშირად), შეგიძლიათ, გამოიყენოთ მეტოქეების შესაძლებლობებზე თქვენთვის ცნობილი ინფორმაცია, უსაფრთხოების წარსული ინციდენტების ანალიზი, სხვა მსგავსი ორგანიზაციების გამოცდილება და, რა თქმა უნდა, თქვენი ორგანიზაციის მიერ მანამდე დანერგილი შედეგების შერბილების რაიმე სტრატეგიის არსებობა.

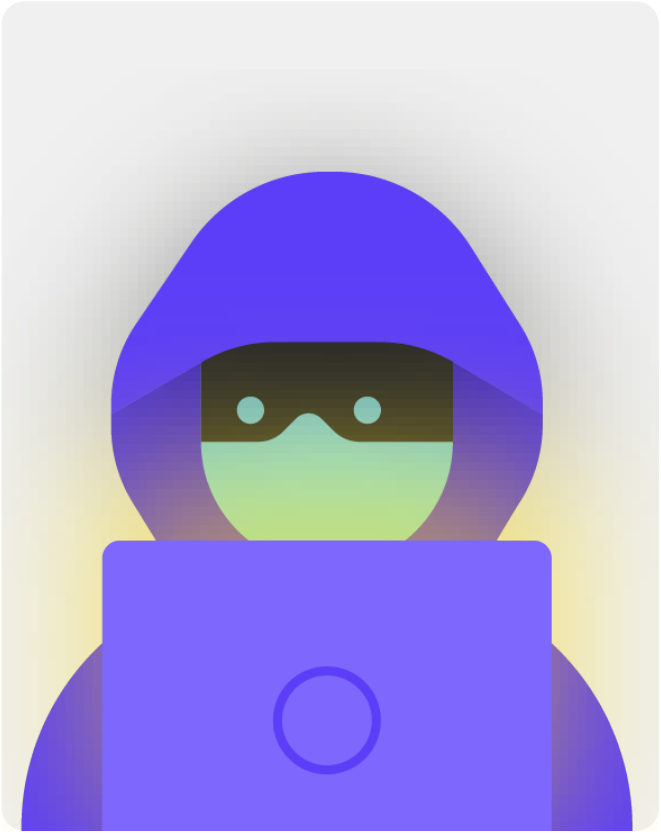
საფრთხის გავლენის გასაზომად დაფიქრდით, როგორი იქნებოდა თქვენი სამყარო საფრთხის რეალურად წარმოშობის შემთხვევაში. დასვით კითხვები, როგორიცაა „როგორ დაგვაზიანა საფრთხემ, როგორც ორგანიზაცია და როგორც ხალხი, ფიზიკურად და მენტალურად?“, „ რამდენად გრძელვადიანი იყო ეფექტი?“, „წარმოშობს ეს სხვა საზიანო სიტუაციებს?“ და „რამდენად ამცირებს ის ჩვენს უნარს, მივაღწიოთ ორგანიზაციულ მიზნებს ახლა და მომავალში?“ ამ კითხვებზე პასუხის შემდეგ დაფიქრდით, როგორია გავლენა: სუსტი, საშუალო თუ ძლიერი.

თქვენი საფრთხეების ალბათობის და გავლენის მიხედვით დალაგების შემდეგ შეგიძლიათ, შეუდგეთ უფრო ინფორმირებული სამოქმედო გეგმის შედგენას. იმ საფრთხეებზე კონცენტრაციით, რომლებიც უფრო სავარაუდოა, რომ წარმოიშვას და რომლებიც იქონიებს მნიშვნელოვან ნეგატიურ გავლენას, თქვენ მიმართავთ თქვენს შეზღუდულ რესურსებს მაქსიმალურად შესაძლო ქმედითი და შედეგიანი მიმართულებით.

თქვენი მუდმივი მიზანია, მაქსიმალურად შეამციროთ რისკი, თუმცა, არავის, მათ შორის რესურსებით მაქსიმალურად უზრუნველყოფილ მთავრობას თუ კომპანიასაც კი, არ შეუძლია რისკების სრულად აღმოფხვრა. და ეს ნორმალურია: შეგიძლიათ გააკეთოთ ბევრი რამ საკუთარი თავის, თქვენი კოლეგების და თქვენი ორგანიზაციის დასაცავად - ყველაზე დიდ საფრთხეებზე ზრუნვით.



რისკების შეფასების ხსენებული პროცესის მართვაში დასახმარებლად, განიხილეთ ისეთი დიაგრამის გამოყენება, როგორიცაა Electronic Frontier Foundation-ის მიერ შემუშავებული ეს დიაგრამა. გახსოვდეთ, რომ ამ პროცესის ფარგლებში თქვენს მიერ შექმნილი ინფორმაცია (როგორიცაა მეტოქეების და მათთან დაკავშირებული საფრთხეების სია) შესაძლოა იყოს სენსიტიური, ამდენად, მნიშვნელოვანი მისი უსაფრთხოების დაცვა.



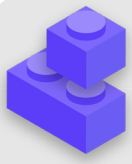
თქვენი ორგანიზაციის კიბერუსაფრთხოების გეგმის შემუშავება

მიუხედავად იმისა, რომ ორგანიზაციების უსაფრთხოების გეგმები მცირედ განსხვავებულად გამოიყურება გამომდინარე მათი რისკების შეფასებიდან და ორგანიზაციული დინამიკიდან, ზოგიერთი საკვანძო კონცეფცია თითქმის უნივერსალურია.

წინამდებარე „სახელმძღვანელო“ ეხება ხსენებულ არსებით კონცეფციებს ისე, რომ დაეხმაროს თქვენს ორგანიზაციას შეიმუშაოს უსაფრთხოების გეგმა პრაქტიკული გადაწყვეტების და რეალურ სამყაროში გამოყენების თვალსაზრისით.

წინამდებარე „სახელმძღვანელო“ უზრუნველყოფს შეთავაზებებს და ოფციებს, რომლებიც უფასო ან მეტად იაფია. გახსოვდეთ, რომ ეფექტური უსაფრთხოების გეგმის რეალიზაციასთან დაკავშირებული ყველაზე დიდი ხარჯი იქნება დრო, რომელიც გესაჭიროებათ თქვენ და თქვენს ორგანიზაციას თქვენი ახალი გეგმის განხილვის, შესწავლის და რეალიზაციისათვის. თუმცა, გამომდინარე თქვენი ორგანიზაციის წინაშე არსებული სავარაუდო რისკებიდან, ხსენებული ინვესტიციის გაწევა ნამდვილად ღირს.

თითოეულ სექციაში შეგხვდებათ იმ საკვანძო საკითხის განმარტება, რომლის თაობაზეც ინფორმირებული უნდა იყოს თქვენი ორგანიზაცია და მისი პერსონალი - ანუ რა არის ის და რატომაა ის მნიშვნელოვანი. თითოეული საკითხი შეწყვილებულია არსებით სტრატეგიებთან, მიდგომებთან და რეკომენდებულ ინსტრუმენტებთან თქვენი რისკის შეზღუდვისათვის, ასევე, რჩევებთან და დამატებით რესურსებზე ბმულებთან, რომლებიც შეიძლება დაგეხმაროთ ხსენებული რეკომენდაციების რეალიზაციაში თქვენს ორგანიზაციაში.



უსაფრთხოების გეგმის საწყისი კომპლექტი

თქვენი ორგანიზაციის დასახმარებლად დაამუშავეთ „სახელმძღვანელოში“ მოცემული გაკვეთილები და აქციეთ ისინი რეალურ გეგმად, ისარგებლეთ მოცემული საწყისი კომპლექტით. კომპლექტი შეგიძლიათ, ამობეჭდოთ ან ციფრულად შეავსოთ ის „სახელმძღვანელოს“ ციფრულ ფორმატში ონლაინ წაკითხვისას. ჩანაწერების გაკეთებისას და თქვენი უსაფრთხოების გეგმის განახლების ან შედგენისას აუცილებლად მიუთითეთ თითოეულ სექციაში მოცემული „უსაფრთხოების გეგმის შემადგენელი ბლოკები“. უსაფრთხოების გეგმა ვერ იქნება სრული, სულ მცირე, ხსენებული არსებითი ელემენტების მითითების გარეშე.



გამოიყენეთ სხვა რესურსები, რომლებიც ასევე შეიძლება დაგეხმაროთ თქვენი გეგმის შედგენაში და რეალიზაციაში. როგორც სამოქალაქო საზოგადოებრივი ორგანიზაციას, უფასო აპი **SOAP** („პოლიტიკის ავტომატიზებული შემუშავების ორგანიზაციების დაცვა“) შეიძლება დაგეხმაროთ თქვენი უსაფრთხოების გეგმის შემუშავების გამარტივებაში და ავტომატიზებაში.

ასევე გამოიყენეთ უფასო ტრენინგ-რესურსები, როგორიცაა Consumer Reports-ის **Security Planner**, **Security First-ის აპი Umbrella**, Free Press Unlimited-ის და Greenhost-ის **Totem-ის პროექტი** და Global Cyber Alliance-ის **„კიბერუსაფრთხოების კომპლექტი მისიის ტიპის ორგანიზაციებისათვის“**, რომლებიც მოიცავს რესურსებს წინამდებარე „სახელმძღვანელოში“ ხსენებული მრავალი აღიარებული პრაქტიკის შესახებ და ბმულებს ტრენინგის ათობით მეთოდიკაზე, რომლებიც დაგეხმრებათ არაერთი საკვანძო საფუძვლის რეალიზაციაში.



უსაფრთხოების კულტურის დანერგვა

უსაფრთხოების კულტურის დანერგვა

მყარი საფუძველი: პროფილების და მოწყობილობების დაცვა

უსაფრთხო კომუნიკაცია და მონაცემების შენახვა

უსაფრთხოების დაცვა ინტერნეტში

ფიზიკური უსაფრთხოების დაცვა

როგორ იქცევით, როცა საქმე ცუდადაა

უსაფრთხოებაში მთავარი ხალხია და თქვენი ორგანიზაციის დასაცავად უნდა დარწმუნდეთ, რომ ყველა მონაწილე სერიოზულად აღიქვამს კიბერუსაფრთხოებას. კულტურის შეცვლა რთულია, თუმცა, რამდენიმე მარტივმა ნაბიჯმა და მნიშვნელოვანმა საუბარმა შეიძლება მყისიერად მიგიყვანოთ ატმოსფერომდე, რომელიც აამოქმედებს თქვენი პერსონალის და ორგანიზაციის კიბერუსაფრთხოების მოქნილ სტრატეგიას უსაფრთხოების წინაშე არსებული საფრთხეების პასუხად. ორგანიზაციული უსაფრთხოების აღნიშნული კულტურის დანერგვის ერთ-ერთი უმარტივესი, მაგრამ, უმნიშვნელოვანესი ნაბიჯია მასზე საუბარი თქვენი ორგანიზაციის ფარგლებში და ხელმძღვანელობის მუდმივად სანიმუშო ქცევა.

მოახდინეთ უსაფრთხოების ინტეგრაცია თქვენს ყოველდღიურ საწარმოო სტრუქტურაში

როგორც ეს დეტალურად აღწერილია [Tactical Tech-ის „ყოვლისმომცველი უსაფრთხოების სახელმძღვანელოში“](), მეტად მნიშვნელოვანია, მუდმივად ვიქონიოთ უსაფრთხო სივრცე უსაფრთხოების სხვადასხვა ასპექტზე სასაუბროდ.

ამგვარად, თუ გუნდის წევრები შეშფოთდებიან უსაფრთხოებასთან დაკავშირებით, ისინი ნაკლებად იღელვებენ თავის პარანოიდად წარმოჩენის ან სხვების დროის გაფლანგვის გამო. **უსაფრთხოების შესახებ რეგულარული საუბრების დაგეგმვა** ასევე ახდენს უსაფრთხოებასთან დაკავშირებულ საკითხებზე ინტერაქციის და ასახვის სიხშირის ნორმალიზებას ისე, რომ არ მოხდეს პრობლემების დავიწყება, ხოლო გუნდის წევრები, დიდი ალბათობით, სულ მცირე, უსაფრთხოების პასიურ ცნობიერებას შეიტანენ თავიანთ საქმიანობაში. არაა აუცილებელი, ეს ყოველკვირეული იყოს, მაგრამ მიეცით მას პერიოდული ხასიათი. აღნიშნული დისკუსიები უნდა იყოს ადგილი არა მხოლოდ ტექნიკური უსაფრთხოების საკითხებისათვის, არამედ იმ პრობლემებისათვის, რომლებიც გავლენას ახდენს პერსონალის კომფორტზე და უსაფრთხოებაზე, როგორიცაა კონფლიქტი საზოგადოებაში, ონლაინ (და ოფლაინ) შევიწროება ან ციფრული ინსტრუმენტების გამოყენების და რეალიზაციის პრობლემები. საუბრები, შესაძლოა, ეხებოდეს ისეთ საკითხებსაც, როგორიცაა ოფლაინ ინფორმაცია - ჩვევების გაზიარება და მეთოდები, რომლებითაც პერსონალი იცავს ან არ იცავს ინფორმაციას სამსახურის მიღმა. ბოლოს და ბოლოს, მნიშვნელოვანია გვახსოვდეს, რომ ორგანიზაციის უსაფრთხოება ძლიერია მისი უსუსტესი რგოლის დონეზე. ერთ-ერთი მეთოდი თანამიმდევრული ჩართულობის მისაღწევად არის უსაფრთხოების შეტანა რეგულარული კრებების დღის წესრიგში. ასევე, შეგიძლიათ, გაუნაწილოთ უსაფრთხოების თაობაზე დისკუსიის ორგანიზების და ფასილიტაციის პასუხისმგებლობა ორგანიზაციის წევრებს, რამაც შესაძლოა წარმოშვას აზრი, რომ უსაფრთხოების დაცვა არის არა მხოლოდ რამდენიმე თანამშრომლის ან IT-გუნდის, არამედ ყველას ვალდებულება. უსაფრთხოების თაობაზე დისკუსიისათვის ოფიციალური ხასიათის მინიჭების შემდეგ პერსონალი, სავარაუდოდ, უფრო კომფორტულად იგრძნობს თავს ხსენებული მნიშვნელოვანი საკითხების საკუთარ წრეში ან ნაკლებად ოფიციალურ გარემოში განხილვისას.

ასევე, მნიშვნელოვანია, ჩავრთოთ უსაფრთხოების ელემენტები ორგანიზაციის ჩვეულ საქმიანობაში, მაგ., ახალი თანამშრომლის მიღებისას ან სისტემებზე წვდომის გაუქმება თანამშრომლის გათავისუფლებისას. უსაფრთხოება არ უნდა იყოს რაღაც „დამატებითი“ წუხილის საგანი, არამედ უნდა იყოს ***თქვენი სტრატეგიის და ოპერაციების განუყოფელი ნაწილი***.

გახსოვდეთ, რომ უსაფრთხოების ყველა გეგმა უნდა განიხილებოდეს ცვალებად დოკუმენტად და უნდა ექვემდებარებოდეს ხელახლა შეფასებას და რეგულარულ განხილვას, განსაკუთრებით, როცა ორგანიზაციას უერთდებიან ახალი თანამშრომლები ან მოხალისეები ან როცა იცვლება თქვენი უსაფრთხოების კონტექსტი.

დაგეგმეთ სტრატეგიის გადახედვა და განახლება ყოველწლიურად ან მაშინ, როცა მნიშვნელოვნად იცვლება სტრატეგია, ინსტრუმენტები ან თქვენ წინაშე არსებული საფრთხეები.

მიიღეთ ორგანიზაციული თანხმობა

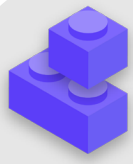
უსაფრთხოების წარმატებული კულტურის ნაწილია ასევე უსაფრთხოების თქვენს გეგმაში თქვენი ორგანიზაციის სრული ჩართულობა.

მეტად მნიშვნელოვანია, რომ აღნიშნული მოიცავდეს ორგანიზაციის ხელმძღვანელობის ხმამაღალ მხარდაჭერას და მითითებებს, რომლებიც ბევრ შემთხვევაში საბოლოო გადაწყვეტილებას მიიღებენ დროის, რესურსების და ენერგიის გამოყოფაზე უსაფრთხოების ეფექტური გეგმის შემუშავების მიზნით. თუ არა ისინი, ამას არც სხვა აღიქვამს სერიოზულად. ორგანიზაციის ხსენებული ჩართულობის მისაღწევად გულდასმით დაფიქრდით, როდის და როგორ წარმოადგინოთ თქვენი გეგმა, გააკეთეთ ეს ნათლად, უზრუნველყავით რომ ხელმძღვანელობა მხარს უჭერდეს თქვენს შეხედულებებს და გააცანით ყველას გეგმის ყველა ელემენტი და ნაბიჯი ისე, რომ თქვენი მიზანი არ იყოს საიდუმლო ან ბუნდოვანი. დღეისათვის არაერთი დონორი ეძებს გრანტების სანაცვლოდ მაღალი დონის უსაფრთხოების შემქმნელებს, ასე რომ, აღნიშნულზე პერსონალის ინფორმირება, შესაძლოა, ასევე კარგი მეთოდი იყოს ორგანიზაციის მაქსიმალური ჩართულობის მისაღწევად. უსაფრთხოებაზე საუბრისას მოერიდეთ შეშინების ტაქტიკას. ხანდახან საფრთხეები, რომელთა წინაშეც თქვენი ორგანიზაცია და პერსონალი დგას, შესაძლოა, საშინელი იყოს, თუმცა, ეცადეთ, ყურადღება გაამახვილოთ ფაქტებზე და კითხვებისათვის მშვიდი გარემოს შექმნაზე. საშიშროების ჭარბ ხიფათად წარმოდგენამ, შესაძლოა, აიძულოს ხალხი, შეგრაცხოს სენსაციების მოყვარულად, ან უბრალოდ დანებდეს, მიიჩნევს რა, რომ რაიმეს გაკეთებას აზრი არა აქვს, რაც სრულიად არ შეესაბამება რეალობას.

შეიმუშავეთ ტრენინგის გეგმა

გეგმის შედგენის და შესრულების დაწყების შემდეგ მოიფიქრეთ, როგორ აწარმოებთ მთელი პერსონალის (და მოხალისეების) ტრენინგს ხსენებული ახალი აღიარებული პრაქტიკის საკითხებზე.

რეგულარული ტრენინგის დაწესება და მასზე დასწრებისათვის და პერსონალზე დაკისრებული მოვალეობების შესრულების შეფასებისათვის აუცილებელი ხასიათის მინიჭება სასარგებლო ტაქტიკა შეიძლება აღმოჩნდეს. მოერიდეთ იმ პერსონალისთვის მკაცრი, ნეგატიური შედეგების შექმნას, რომლებიც უსაფრთხოების კონცეფციას ეურჩებიან. გახსოვდეთ, რომ პერსონალის ნაწილმა სხვებისაგან განსხვავებულად შეიძლება მოახდინოს ადაპტაცია და ტექნოლოგიების შესწავლა გამომდინარე ციფრული ინსტრუმენტების და ინტერნეტის ცოდნის სხვადასხვა დონიდან. წარუმატებლობის შიში მხოლოდ კიდევ უფრო ამუხრუჭებს პერსონალს პრობლემებზე ინფორმირების თუ დახმარების მიღების თვალსაზრისით. თუმცა, პოზიტიური ანგარიშვალდებულების და ჯილდოების დაწესება ტრენინგის წარმატებულად გავლისათვის და პოლიტიკების ჩამოყალიბება, შესაძლოა, დაგეხმაროთ ორგანიზაციაში სტიმულირების გაუმჯობესებაში. სხვა ღირებული მხარდაჭერა შეგიძლიათ, მიიღოთ ციფრული უსაფრთხოების საკითხებზე ტრენინგის ადგილობრივი ან საერთაშორისო ქსელებიდან და ტრენინგის უფასო რესურსებიდან, როგორიცაა Security First-ის აპი Umbrella Free Press Unlimited-ის და Greenhost-ის Totem-ის პროექტი Global Cyber Alliance-ის სასწავლო პორტალი.



უსაფრთხოების კულტურის დანერგვა

- **დაგეგმეთ რეგულარული საუბრები და ტრენინგი უსაფრთხოების და თქვენი უსაფრთხოების გეგმის შესახებ.**
- **ჩართეთ ყველა – გაანაწილეთ პასუხისმგებლობა თქვენი უსაფრთხოების გეგმის შესრულებაზე მთელს ორგანიზაციაში.**
- **უზრუნველყავით, რომ ხელმძღვანელობა უსაფრთხოების საკითხებში კარგი ქცევისა და გეგმის შესრულების მაგალითი იყოს.**
- **მოერიდეთ დაშინების ტაქტიკას ან დასჯას – წაახალისეთ პროგრესი და შექმენით კომფორტული სივრცე პერსონალის მიერ პრობლემებზე ინფორმირების და დახმარების მიღებისათვის.**
- **განაახლეთ თქვენი უსაფრთხოების გეგმა ყოველწლიურად ან ორგანიზაციაში მნიშვნელოვანი ცვლილებების შემდეგ.**



მყარი საფუძველი: პროფილების და მოწყობილობების დაცვა

რისთვისაა საჭირო კონცენტრაცია ანგარიშებსა და მოწყობილობებზე? რადგან ისინი ქმნის იმ ყველაფრის საფუძველს, რასაც აკეთებს თქვენი ორგანიზაცია ციფრულად.

თქვენ თითქმის უსათუოდ გაქვთ წვდომა სენსიტიურ ინფორმაციაზე, აწარმოებთ შიდა და გარე კომუნიკაციას და ინახავთ მათზე პირად ინფორმაციას. თუ ისინი დაუცველია, ეს ყველაფერი და მეტიც რისკის ქვეშ შეიძლება აღმოჩნდეს. მაგალითად, თუ ჰაკერები უთვალთვალებენ კლავიატურაზე თქვენს მუშაობას ან უსმენენ თქვენს მიკროფონს, ისინი ხელში ჩაიგდებენ კოლეგებთან თქვენს კერძო საუბრებს მიუხედავად იმისა, რამდენად დაცულია თქვენი შეტყობინებების აპლიკაცია ან, თუ მეტოქეები მოიპოვებენ წვდომას თქვენი ორგანიზაციის ანგარიშებზე სოციალურ მედიაში, მათ შეეძლებათ, მარტივად დააზიანონ თქვენი რეპუტაცია და საიმედოობა და ძირი გამოუთხარონ თქვენს წარმატებულ მუშაობას. ამდენად, როგორც ორგანიზაციამ, მნიშვნელოვანია, უზრუნველყოთ რომ ყველა იღებდეს მარტივ, მაგრამ ეფექტურ ზომებს საკუთარი მოწყობილობების და ანგარიშების დასაცავად. აღსანიშნავია, რომ ეს რეკომენდაციები ასევე მოიცავს პირად ანგარიშებსა და მოწყობილობებს, რადგან ისინი ხშირად ადვილი სამიზნეა მტრულად განწყობილი მხარეებისთვის. ჰაკერები სიამოვნებით უთვალთვალებენ ადვილ სამიზნეს და ტეხენ პირად ანგარიშს ან სახლის კომპიუტერს, თუ თქვენი გუნდი იყენებს მათ კომუნიკაციისა და მნიშვნელოვან ინფორმაციაზე წვდომისათვის.



დაიცავით ანგარიშები და სამოქალაქო საზოგადოება

ფართოდ გაშუქებული SolarWinds-ის 2020 წლის ბოლოს გამოვლენილი გატეხა, რომელმაც დააზარალა 250-ზე ორგანიზაცია, მათ შორის, შეერთებული შტატების სამთავრობო დეპარტამენტები Microsoft-ის და Cisco-ს მსგავსი ტექნოლოგიის მიმწოდებლები და არასამთავრობო ორგანიზაციები, ნაწილობრივ გამოწვეული იყო მარტივი პაროლების, რომლებიც გამოიყენებოდა მნიშვნელოვან ადმინისტრაციულ პროფილებში. ჯამში, გატეხასთან დაკავშირებული დარღვევების 80%-მდე მოხდა სუსტი ან ხელახლა გამოყენებული პაროლების გამო.

ხსენებულის მსგავსი პაროლების გატეხის მზარდი რაოდენობის და ყველა სახის მეტოქისათვის რთული პაროლების გასატეხი ინსტრუმენტების მარტივი ხელმისაწვდომობის ფონზე, პაროლის დადების აღიარებული პრაქტიკა და ორფაქტორიანი ავთენტიკაცია წარმოადგენს აუცილებლობას სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის. სამოქალაქო საზოგადოების ანგარიშებზე შეტევის ერთი მაგალითი გამოვლინდა Facebook-ის მიერ 2020 წელს. მათი ანგარიშის თანახმად, ბანგლადეშელი ჰაკერების ჯგუფებმა შეტევა მიიტანეს ადგილობრივი სამოქალაქო საზოგადოების აქტივისტების, ჟურნალისტებისა და რელიგიური უმცირესობების პროფილებზე.სამწუხაროდ, ჰაკერებმა შეძლეს Facebook-ის ხსენებული ანგარიშების, მათ შორის, Facebook-ში ადგილობრივი ჯგუფის გვერდის ადმინისტრატორის ანგარიშის წარმატებით გატეხა. მიიღეს რა წვდომა ადმინისტრატორის ანგარიშზე, ჰაკერებმა წაშალეს დანარჩენი ადმინისტრატორები, ხელში ჩაიგდეს და გააუქმეს გვერდი, რითაც ხელი შეუშალეს ჯგუფს საკვანძო ინფორმაციის გაზიარებაში და საკუთარ აუდიტორიასთან კომუნიკაციაში.Facebook-ის გამოძიებამ დაადგინა, რომ ანგარიშები, სავარაუდოდ, გატეხეს სხვადასხვა საშუალებით, მათ შორის, ანგარიშის აღდგენის ფუნქციის ბოროტად გამოყენებით.ანგარიშებში ორფაქტორიანი ავთენტიკაცია რომ ყოფილიყო გამოყენებული, აღნიშნული შეტევა გაცილებით რთული იქნებოდა ჰაკერებისათვის შედეგიანად შესრულების თვალსაზრისით.



დოკუმენტაციის დაცვა or დაცულობა პაროლები და აუთენტურობის ორფაქტორული შემოწმება

დღევანდელ სამყაროში მოსალოდნელია, რომ თქვენს ორგანიზაციას და მის პერსონალს ჰქონდეს ათობით, თუ არა ასობით, ანგარიში, რომლებიდანაც, გატეხვის შემთხვევაში, შესაძლოა, ხელმისაწვდომი გახდეს სენსიტიური ინფორმაცია ან წარმოიშვას პიროვნებებისათვის ზიანის რისკიც კი.

იფიქრეთ სხვადასხვა ანგარიშზე, რომლებიც შეიძლება ჰქონდეთ პერსონალის წევრებს და მთლიანად ორგანიზაციას: ელფოსტა, სასაუბრო აპლიკაციები, სოციალური მედია, ონლაინ-ბანკინგი, მონაცემთა დისტანციური საცავი, ასევე, ტანსაცმლის მაღაზიები, ადგილობრივი რესტორნები, გაზეთები და მრავალი სხვა ვებსაიტი თუ აპლიკაცია, რომელთა სისტემებშიც შედიხართ. მაღალი დონის უსაფრთხოება დღევანდელ სამყაროში საჭიროებს გულდასმით მიდგომას თავდასხმებისგან ყველა ხსენებული პროფილის დასაცავად. ეს იწყება მთელს ორგანიზაციაში პაროლების ჰიგიენისა და ორფაქტორიანი ავთენტიკაციის დანერგვით.

როგორია კარგი პაროლი?

კარგ, ძლიერ პაროლს განაპირობებს სამი ფაქტორი: სიგრძე, ნებისმიერობა და უნიკალურობა.

სიგრძე

რაც უფრო გრძელია პაროლი, მით რთულია მეტოქის მიერ მისი გამოცნობა. დღეისათვის პაროლების გატეხვის უმეტესობა სრულდება კომპიუტერული პროგრამებით და ხსენებულ მანკიერ პროგრამებს დიდი დრო არ სჭირდება მოკლე პაროლის გასატეხად. ამიტომ, მნიშვნელოვანია, რომ თქვენი პაროლები მოიცავდეს მინიმუმ 16 სიმბოლოს ან მინიმუმ ხუთ სიტყვას და უკეთესია, უფრო გრძელიც იყოს.

ნებისმიერობა

პაროლი გრძელიც რომ იყოს, არ არის კარგი, თუ არის რაიმე, რაც ადვილად შეიძლება გამოიცნოს მეტოქემ თქვენ შესახებ. მოერიდეთ თქვენი დაბადების დღის, მშობლიური ქალაქის, საყვარელი საქმის თუ იმ სხვა ფაქტების გამოყენებას, რომლებიც შეიძლება ვინმემ გაარკვიოს თქვენ შესახებ ინტერნეტში სწრაფი ძიებით.

უნიკალურობა

სავარაუდოდ, პაროლის გამოყენების „ყველაზე ცუდი მეთოდია“ ერთი და იმავე პაროლის გამოყენება სხვადასხვა საიტისთვის.პაროლების გამეორება დიდი პრობლემაა, რადგან ეს ნიშნავს, რომ ხსენებული ანგარიშებიდან მხოლოდ ერთის გატეხისას იმავე პაროლის გამოყენებით მოწყვლადი ხდება სხვა ანგარიშებიც.თუ არაერთ საიტზე იყენებთ ერთსა და იმავე კოდურ ფრაზას, ამით მნიშვნელოვნად იზრდება ერთი შეცდომის თუ მონაცემთა უსაფრთხოების დარღვევის გავლენა.შესაძლოა, არ დარდობდეთ, თუ რა პაროლი გაქვთ ადგილობრივ ბიბლიოთეკაში, თუმცა მისი გატეხის და უფრო სენსიტიურ ანგარიშში გამოყენების შემთხვევაში, მნიშვნელოვანი ინფორმაცია შეიძლება მოიპარონ.



სიგრძის, ნებისმიერობის და უნიკალურობის ხსენებული მიზნის მიღწევის ერთი მარტივი გზაა, აირჩიოთ სამი ან ოთხი ცნობილი, მაგრამ შემთხვევითი სიტყვა. მაგალითად, თქვენი პაროლი შეიძლება იყოს „ყვავილი სანათი მწვანე დათვი“, რომლის დამახსოვრება ადვილია, მაგრამ გამოცნობა ძნელი. შეგიძლიათ, დაათვალიეროთ Better Buys-ის ვებსაიტი და გაეცნოთ პროგნოზს, რამდენად სწრაფად შეიძლება სუსტი პაროლის გატეხვა.

დახმარებისათვის გამოიყენეთ პაროლების მენეჯერი

ამგვარად, იცით, რომ ორგანიზაციის ყველა წევრისათვის მნიშვნელოვანია, გამოიყენონ გრძელი, შემთხვევითი და განსხვავებული პაროლები თითოეული პირადი და ორგანიზაციული ანგარიშისთვის, მაგრამ როგორ უნდა გააკეთოთ ეს რეალურად? კარგი პაროლის ათობით (თუ არა ასობით) ანგარიშისათვის დამახსოვრება შეუძლებელია. ამიტომ, ეშმაკობს ყველა. არასწორია ამისათვის პაროლის ხელახლა გამოყენება. საბედნიეროდ, ნაცვლად ამისა, შეგვიძლია, მივმართოთ პაროლების მენეჯერს, რომ გავიმარტივოთ სიცოცხლე (და უზრუნველვყოთ პაროლების ჩვენეული პრაქტიკის დაცვა). ხსენებულ აპლიკაციებს, რომელთაგან არაერთზე წვდომა შესაძლებელია კომპიუტერით ან მობილური ტელეფონით შეუძლია, თქვენთვის და მთელი თქვენი ორგანიზაციისათვის შექმნას, შეინახოს და მართოს პაროლები. უსაფრთხო პაროლების მენეჯერის გამოყენება გულისხმობს, რომ უნდა გახსოვდეთ მხოლოდ ერთი მეტად ძლიერი, გრძელი პაროლი, რომელსაც პირველადი პაროლი (ისტორიულად კი „მთავარი“ პაროლი) ეწოდება და ამავდროულად, ისარგებლებთ კარგი, უნიკალური პაროლებით ყველა თქვენი ანგარიშისთვის. ხსენებულ პირველად პაროლს (და, იდეალურ შემთხვევაში, ორფაქტორიან ავთენტიკაციას (2FA), რომელიც განიხილება შემდეგ სექციაში) გამოიყენებთ თქვენი პაროლების მენეჯერის გასახსნელად და თქვენს ყველა სხვა პაროლზე წვდომის მისაღებად. პაროლების მენეჯერები, შესაძლოა, ასევე გავრცელებული იქნეს რამდენიმე პროფილზე ორგანიზაციაში დაცული პაროლების გაზიარების გამარტივების მიზნით.

რატომ გვჭირდება რაღაც ახლის გამოყენება? არ შეგვიძლია, უბრალოდ ჩამოვწეროთ ისინი ქაღალდზე ან კომპიუტერულ ცხრილში?

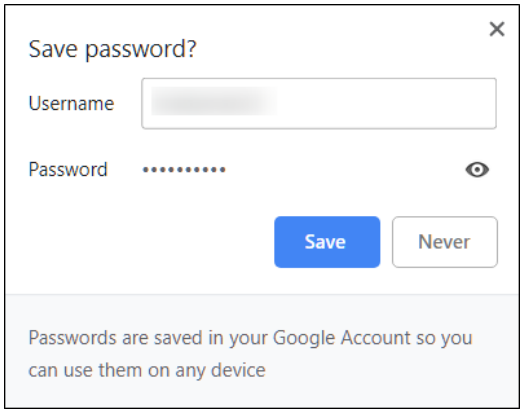
სამწუხაროდ, არსებობს მრავალი გავრცელებული მიდგომა პაროლების მართვისადმი, რომლებიც არაა უსაფრთხო. ქაღალდის ფურცლებზე პაროლების შენახვამ შენახვამ (თუ არ ინახავთ მათ სეიფში ჩაკეტილს), შესაძლოა, დაუქვემდებაროს ისინი ფიზიკურ ქურდობას, ცნობისმოყვარე თვალს და უბრალოდ დაკარგვას ან დაზიანებას. პაროლების კომპიუტერულ დოკუმენტში შენახვა მეტად უმარტივებს წვდომის მოპოვებას ჰაკერებს – ან ვინმეს, ვინც მოიპარავს თქვენს კომპიუტერს არა მხოლოდ თქვენი მოწყობილობის დასაუფლებლად, არამედ თქვენს ყველა პროფილზე წვდომისათვის. კარგი პაროლების მენეჯერის გამოყენება ისევე ადვილია, როგორც ხსენებული დოკუმენტის, მაგრამ უფრო უსაფრთხოა.

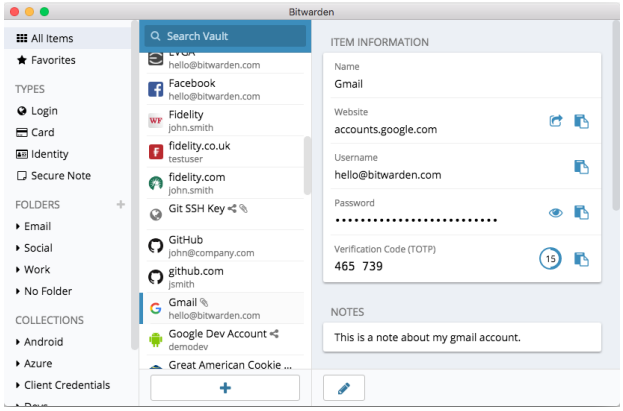
რატომ უნდა ვენდოთ პაროლების მენეჯერს?

პაროლების ხარისხიან მენეჯერებში სისტემების უსაფრთხოების დასაცავად გამოიყენება უჩვეულო სიგრძის პაროლები (და მუშაობენ უსაფრთხოების საუკეთესო გუნდები). პაროლების მართვის კარგი აპლიკაციები (რამდენიმე რეკომენდებულია ქვემოთ) ასევე გამართულია ისე, რომ არ გააჩნია თქვენი პროფილების „გახსნის“ უნარი. აღნიშნული ნიშნავს, რომ უმეტეს შემთხვევაში, მათი გატეხის ან ინფორმაციის გადაცემის მიზნით ლეგალურად იძულებისას, მათ არ შეუძლიათ თქვენი პაროლების დაკარგვა ან გაცხადება. ასევე მნიშვნელოვანია, გახსოვდეთ, რომ არსებობს განუსაზღვრელად მეტი ალბათობა იმისა, რომ მეტოქემ გამოიცნოს თქვენი რომელიმე სუსტი ან განმეორებადი პაროლი ან აღმოაჩინოს ის საჯარო მონაცემების არასანქცირებული მიღებით, ვიდრე მოხდეს კარგი პაროლების მენეჯერის უსაფრთხოების სისტემების გატეხა. მნიშვნელოვანია, იყოთ სკეპტიკური და, რა თქმა უნდა, ბრმად არ უნდა ენდოთ ნებისმიერ პროგრამულ უზრუნველყოფას და აპლიკაციას, მაგრამ პაროლების სანდო მენეჯერს გააჩნია ყველა მართებული სტიმული სწორად მუშაობისთვის.



ნაცვლად თქვენი ბრაუზერის გამოყენებისა (როგორიცაა Chrome-ი, ნაჩვენები მარცხნივ) პაროლების შესანახად, გამოიყენეთ სპეციალური პაროლების დისპეტჩერი (მაგალითად, Bitwarden-ი, ნაჩვენები მარჯვნივ). პაროლების დისპეტჩერებს გააჩნია ფუნქცია, აქციოს თქვენი ორგანიზაციის ყოფა უფრო უსაფრთხოდ და კომფორტულად.





რას იტყვით პაროლების ბრაუზერში შენახვაზე?

პაროლების თქვენს ბრაუზერში შენახვა არ არის იგივე, რაც დაცული პაროლების მენეჯერის გამოყენება. ერთი სიტყვით, დაუშვებელია პაროლების მენეჯერად Chrome-ის, Firefox-ის, Safari-ს თუ ნებისმიერი სხვა ბრაუზერის გამოყენება. მიუხედავად იმისა, რომ ეს, რა თქმა უნდა, უკეთესია, ვიდრე მათი ქაღალდზე ან კომპიუტერულ ცხრილში ჩაწერა, თქვენი ვებბრაუზერის მიერ პაროლების შენახვის ფუნქცია უსაფრთხოების თვალსაზრისით მიუღებელია. აღნიშნული ნაკლოვანებები ასევე გართმევთ კომფორტს, რომელიც თან სდევს კარგ პაროლების მენეჯერს. კომფორტის დანაკარგი ამაღლებს ალბათობას, რომ ხალხი თქვენს ორგანიზაციაში განაგრძობს სუსტი პაროლების შედგენის და გაზიარების პრაქტიკას.

მაგალითად, განსხვავებით სპეციალური პაროლების მენეჯერებისაგან, ბრაუზერების საკუთარი „ამ პაროლის შენახვის“ ან „ამ პაროლის დამახსოვრების“ ფუნქციები არ უზრუნველყოფს მარტივ მობილურ თავსებადობას, მუშაობას სხვა ბრაუზერებში და კარგი პაროლის გენერაციას და კონტროლის ინსტრუმენტებს. ხსენებული ფუნქციები წარმოადგენს სპეციალური პაროლების მენეჯერის მნიშვნელოვან შემადგენელ ნაწილს, რომელიც ასე სასარგებლოა თქვენი ორგანიზაციის უსაფრთხოებისათვის. პაროლების მენეჯერი ასევე მოიცავს ორგანიზაციისათვის სპეციფიკურ ფუნქციებს (როგორიცაა პაროლის გაზიარება), რომლებიც უზრუნველყოფს არა მხოლოდ ინდივიდუალურ უსაფრთხოებას, არამედ მთელი თქვენი ორგანიზაციის უსაფრთხოებასაც. თუ პაროლებს თქვენს ბრაუზერში ინახავდით (გამიზნულად ან უნებლიედ), ნუ დაიზარებთ, წაშალოთ ისინი.

რომელი პაროლების მენეჯერი უნდა გამოვიყენოთ?

არსებობს არაერთი კარგი პაროლების მენეჯერი, რომელთა დაყენებაც 30 წუთზე ნაკლებ დროში შეიძლება. თუ ეძებთ სანდო ონლაინ-ვარიანტს თქვენი ორგანიზაციისათვის, რომელზე წვდომაც ნებისმიერ დროს შეეძლება ხალხს არაერთი მოწყობილობიდან, სათანადოდ მხარდაჭერილი და რეკომენდებულია **1Password** (იწყება ერთ მომხმარებელზე თვეში 2,99 აშშ დოლარიდან) ან უფასო, ღია კოდის მქონე **Bitwarden.** Bitwarden-ის მსგავსი ონლაინ-ვარიანტი, შესაძლოა, შესანიშნავი იყოს როგორც უსაფრთხოების, ისე კომფორტულობის მხრივ. Bitwarden, მაგალითად, დაგეხმარებათ, შექმნათ ძლიერი უნიკალური პაროლები და იქონიოთ წვდომა პაროლებზე არაერთი მოწყობილობიდან ბრაუზერით თუ

მობილურის აპლიკაციით. Bitwarden-ის ფასიანი ვერსია (10 აშშ დოლ. წელიწადში) ასევე გვატყობინებს ხელახლა გამოყენებულ, სუსტ ან სავარაუდოდ გატეხილ პაროლებზე, რათა იყოთ ყველა გარემოების საქმის კურსში. პირველადი პაროლის (ასევე ცნობილია, როგორც მთავარი პაროლი) შექმნის შემდეგ უნდა ჩართოთ ორფაქტორიანი ავთენტიკაციაც, რომ მაქსიმალურად იყოს დაცული თქვენი პაროლების მენეჯერის საცავი.

მაღალი დონის უსაფრთხოების წარმართვა ასევე მნიშვნელოვანია **პაროლების მენეჯერის გამოყენებისას.** მაგალითად, თუ იყენებთ თქვენი პაროლების მენეჯერის ბრაუზერის გაფართოებას ან შედიხართ Bitwarden-ის (ან ნებისმიერი სხვა პაროლების მენეჯერის) სისტემაში მოწყობილობიდან, არ დაგავიწყდეთ სისტემიდან გამოსვლა გამოყენების შემდეგ, თუ ხსენებულ აპარატს იზიარებთ სხვასთან ან მიგაჩნიათ, რომ, შესაძლოა, იდგეთ მოწყობილობის ფიზიკური ქურდობის მომატებული რისკის წინაშე. ხსენებული მოიცავს თქვენი პაროლების მენეჯერის სისტემიდან გამოსვლას, თუ ტოვებთ კომპიუტერს ან მობილურს ყურადღების გარეშე. თუ პაროლებს მთელს თქვენ ორგანიზაციაში აზიარებთ, გააუქმეთ პაროლებზე წვდომა (და შეცვალეთ თავად ისინი) ორგანიზაციიდან ხალხის წასვლის შემთხვევაში. მაგალითად, თქვენ არ უნდა გსურდეთ, რომ ყოფილმა თანამშრომელმა შეინარჩუნოს წვდომა თქვენი ორგანიზაციის Facebook-ის პაროლზე.

რა ხდება, თუ ვინმეს დაავიწყდა მისი პირველადი პაროლი?

თქვენი პირველადი პაროლის დამახსოვრება მნიშვნელოვანია. პაროლების მართვის კარგი სისტემები, როგორიცაა ზემოთ რეკომენდებული, არ იმახსოვრებს თქვენს პირველად პაროლს და არც მისი ელფოსტით შეცვლის საშუალებას გაძლევთ ისე, როგორც ვებსაიტებზე.ეს უსაფრთხოების მაღალი დონის ფუნქციაა, მაგრამ ასევე იძულებულს გხდით, დაიმახსოვროთ თქვენი პირველადი პაროლი პაროლების მენეჯერის დაყენების შემდეგ. ამ საკითხში დასახმარებლად, პაროლების დისპეტჩერის პაროლის პირველად შექმნისას, შეგიძლიათ, დააყენოთ ყოველდღიური შეხსენება თქვენი პირველადი პაროლისათვის.



მნიშვნელოვანი: პაროლების დისპეტჩერის გამოყენება თქვენი ორგანიზაციისათვის

შეგიძლიათ, გააუმჯობესოთ მთელს თქვენს ორგანიზაციაში დანერგილი პაროლების პრაქტიკა და უზრუნველყოთ რომ პერსონალის ყველა ცალკეულ წევრს გააჩნდეს წვდომა პაროლების მენეჯერზე (და იყენებდეს მას) მისი მთელს ორგანიზაციაში დანერგვით. ნაცვლად პერსონალის ყველა ცალკეული წევრის მიერ საკუთარის შექმნისა, იფიქრეთ „გუნდურ“ ან „ბიზნეს“ გეგმაში ინვესტიციაზე. მაგალითად, Bitwarden-ის „გუნდის ორგანიზაციული“ გეგმა ერთ მომხმარებელზე 3 $ ღირს თვეში. მის (ან 1Password-ის მსგავსი პაროლების მენეჯერის მსგავსი სხვა გუნდური გეგმის) ხარჯზე გიჩნდებათ უნარი, მართოთ მთელს ორგანიზაციაში გაზიარებული ყველა პაროლი. ორგანიზაციული პაროლების დისპეტჩერის ფუნქციები უზრუნველყოფს არა მხოლოდ მეტ უსაფრთხოებას, არამედ კომფორტსაც პერსონალისთვის. შეგიძლიათ, უსაფრთხოდ გაუზიაროთ სხვადასხვა სამომხმარებლო ანგარიშს პაროლების მენეჯერზე წვდომის პარამეტრები. ხოლო Bitwarden-ს, მაგალითად, ასევე გააჩნია ტექსტის და ფაილის აბონენტთაშორისი დაშიფვრის მოსახერხებელი ფუნქცია, რომელსაც, მისი გუნდური გეგმის ფარგლებში Bitwarden Send ეწოდება. თქვენს ორგანიზაციას ორივე ხსენებული ფუნქცია აძლევს მეტი კონტროლის საშუალებას იმასთან დაკავშირებით, თუ ვის შეუძლია, ნახოს და გააზიაროს რომელიმე პაროლი და გთავაზობთ უფრო მეტად დაცულ ვარიანტს ავტორიზაციის მონაცემების გასაზიარებლად გუნდური ან ჯგუფური ანგარიშებისთვის. თუ გამართავთ პაროლების ორგანიზაციულ მენეჯერს, სპეციალურად დაავალეთ ვინმეს პერსონალის ანგარიშების წაშლა და გაზიარებული პაროლების შეცვლა გუნდიდან ვინმეს წასვლის შემთხვევაში.

რა არის ორფაქტორიანი ავთენტიკაცია?

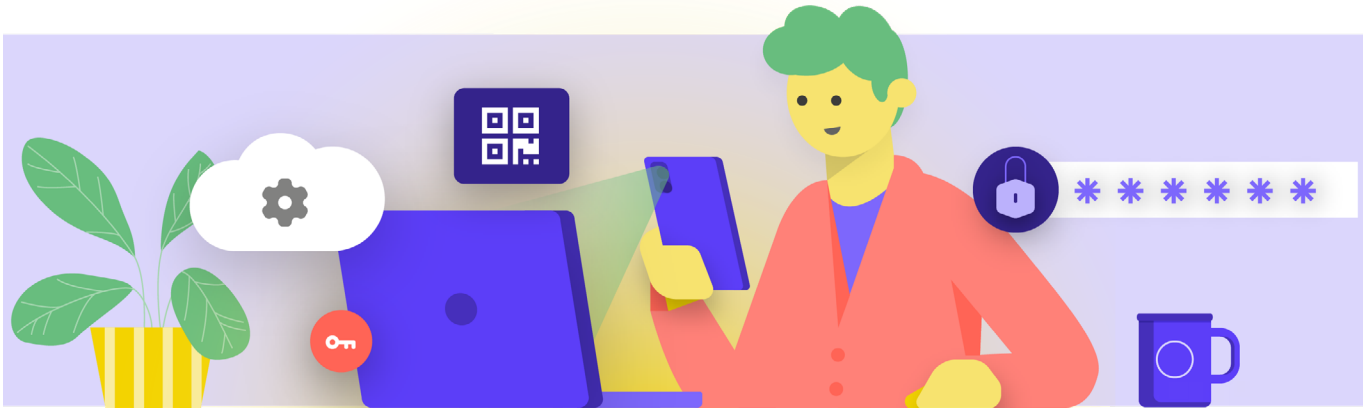
მიუხედავად პაროლების კულტურისა, ჰაკერებისათვის ჩვეული ამბავია პაროლებისთვის გვერდის ავლა. დღევანდელ სამყაროში თქვენი ანგარიშებისთვის საყოველთაო საფრთხეების არიდება დაცვის კიდევ ერთ შრეს საჭიროებს.სწორედ აქ ერთვება მრავალფაქტორიანი და ორფაქტორიანი ავთენტიკაცია – ასევე ცნობილია, როგორც MFA ან 2FA. არსებობს არაერთი მშვენიერი სახელმძღვანელო და რესურსი, სადაც ახსნილია ორფაქტორიანი ავთენტიკაცია, მათ შორისაა Martin Shelton-ის სტატია „ორფაქტორიანი ავთენტიკაცია დამწყებთათვის“ და Center for Democracy &Technology-ს ცნობარი „არჩევნების კიბერუსაფრთხოება 101“. მოცემული სექცია მნიშვნელოვნად ეფუძნება ორივე აღნიშნულ რესურსს, რათა უკეთ იქნას ახსნილი, რატომაა 2FA-ს დანერგვა თქვენს ორგანიზაციაში ასე მნიშვნელოვანი. ერთი სიტყვით, ერთი სიტყვით, 2FA აამაღლებს ანგარიშის დაცულობას, მოითხოვს რა წვდომის მისაღებად მეორად ინფორმაციას – რაღაც მეტს, ვიდრე მხოლოდ პაროლს. მეორადი ინფორმაცია, ჩვეულებრივ, არის რაღაც ისეთი, როგორიცაა აპლიკაციის კოდი თქვენს ტელეფონში, ფიზიკური ნიშანი ან გასაღები. ხსენებული მეორადი ინფორმაცია ასრულებს დაცვის მეორე შრის როლს. თუ ჰაკერი მოიპარავს თქვენს პაროლს ან მიიღებს წვდომას მასზე სხვა პაროლებთან ერთად მონაცემების არასანქცირებული მიღებით, ეფექტურ 2FA-ს შეუძლია, არ დაუშვას ის თქვენს პროფილზე (და ამდენად, პირად და სენსიტიურ ინფორმაციაზე). გადამწყვეტი მნიშვნელობისაა იმის უზრუნველყოფა, რომ ორგანიზაციის ყველა წევრმა გამოიყენოს 2FA საკუთარ ანგარიშებზე.

როგორ დავაყენოთ ორფაქტორიანი ავთენტიკაცია?

არსებობს 2FA-ს დაყენების სამი გავრცელებული მეთოდი: დამცავი გასაღებები, ავთენტიკაციის აპლიკაციები და ერთჯერადი SMS-კოდები.

დამცავი გასარებები

დამცავი გასაღებები წარმოადგენს საუკეთესო შესაძლებლობას გარკვეულწილად იმიტომ, რომ ისინი თითქმის სრულად შეუვალია ფიშინგისათვის. აღნიშნული „გასაღებები“ წარმოადგენს აპარატულ გასაღებებს (წარმოიდგინეთ მინი USB-მოწყობილობა), რომელიც შეიძლება მიაბათ გასაღებების ასხმას (ან იყოს თქვენს კომპიუტერში) მარტივი წვდომისა და დაცულობისთვის. როცა დგება კონკრეტული ანგარიშის გასახსნელად გასაღების გამოყენების დრო, უბრალოდ ათავსებთ მას თქვენს მოწყობილობაში და ფიზიკურად დააწვებით მას, როცა ეს მოგეთხოვებათ სისტემაში შესვლისას. არსებობს მოდელების ფართო სპექტრი, რომელიც შეგიძლიათ, იყიდოთ ონლაინ (20-50 $), მათ შორის, მაღალი შეფასების მქონე YubiKeys. „ნიუ-იორკ ტაიმსის“ Wirecutter-ში არის სასარგებლო ცნობარი არაერთი რეკომენდაციით გასაღების შერჩევის თაობაზე. გახსოვდეთ, რომ ერთი და იგივე დამცავი გასაღები, შესაძლოა, გამოყენებული იქნეს თქვენთვის სასურველი რაოდენობის პროფილებისთვის. რამდენადაც დამცავი გასაღებები ძვირი სიამოვნებაა მრავალი ორგანიზაციისათვის, პროგრამები, როგორიცაა Google-ის გაფართოებული დაცვის პროგრამა თუ Microsoft-ის AccountGuard-ი აღნიშნულ გასაღებებს უფასოდ გადასცემს დადასტურებული რისკის ქვეშ მყოფ ჯგუფებს. მიმართეთ მათ, ვინც გადმოგცათ სახელმძღვანელო, რომ გაარკვიოთ, შეუძლიათ თუ არა თქვენი დაკავშირება ამ პროგრამებთან ან მოგვწერეთ მისამართზე cyberhandbook@ndi.org.



აუთენტურობის აპები

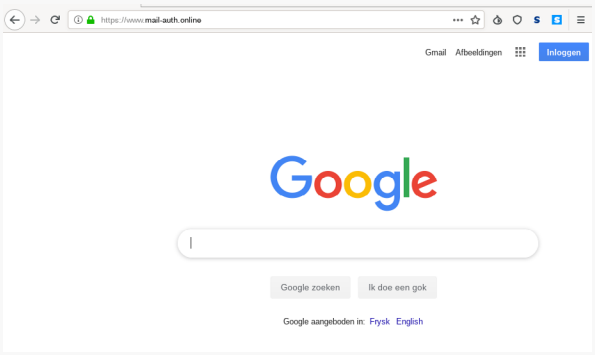
მეორე საუკეთესო ვარიანტი 2FA-სთვის არის ავთენტიკაციის აპლიკაციები. აღნიშნული საშუალებას გაძლევთ მიიღოთ სისტემაში შესვლის დროებითი ორფაქტორიანი კოდი მობილურის აპლიკაციით ან საინფორმაციო შეტყობინება თქვენს სმარტფონზე. პოპულარული და სანდო ვარიანტები მოიცავს Google Authenticator-ს, Authy-ს და Duo Mobile-ს. ავთენტიკაციის აპლიკაციები ასევე დიდებულია, რადგან ისინი მუშაობს მაშინაც, როცა არ გაქვთ წვდომა თქვენს ფიჭურ ქსელზე და უფასოა ფიზიკური პირებისათვის. თუმცა, ავთენტიკაციის აპლიკაციები უფრო მოწყვლადია ფიშინგის მიმართ, ვიდრე დამცავი გასაღებები, რადგან მომხმარებლებს, შესაძლოა, ყალბ ვებსაიტებზე მოტყუებით ჩააწერინონ ავთენტიკაციის აპლიკაციის დამცავი კოდები. სისტემაში შესვლის კოდები ჩაწერეთ მხოლოდ ლეგიტიმურ ვებგვერდებზე. და ნუ „დაადასტურებთ“ სისტემაში შესვლის საინფორმაციო შეტყობინებებს, თუ არ ხართ დარწმუნებული, რომ მოითხოვეთ სისტემაში შესვლა. ავთენტიკაციის აპლიკაციის გამოყენებისას ასევე მნიშვნელოვანია, მზად გქონდეთ სათადარიგო კოდები (განხილულია ქვემოთ) თქვენი ტელეფონის დაკარგვის ან ქურდობის შემთხვევაში.

კოდები SMS-ით

2FA-ს ყველაზე დაუცველი, მაგრამ სამწუხაროდ ყველაზე გავრცელებული ფორმაა SMS-ით კოდების გაგზავნა. რამდენადაც SMS, შესაძლოა, იქნეს ხელში ჩაგდებული, ხოლო ტელეფონის ნომერი – იმიტირებული ან გატეხილი თქვენი მობილური ოპერატორის მეშვეობით, SMS ჯერ კიდევ მიუღებელია, როგორც 2FA-ს კოდების მოთხოვნის მეთოდი.ეს უკეთესია, ვიდრე მხოლოდ პაროლის გამოყენება, მაგრამ რეკომენდებულია ავთენტიკაციის აპლიკაციების ან ფიზიკური უსაფრთხოების გასაღებების გამოყენება, როცა კი ეს შესაძლებელია. გაბედულმა მეტოქემ, შესაძლოა, მიიღოს წვდომა SMS-ით გაგზავნილ 2FA-ს კოდებზე, ჩვეულებრივ, უბრალოდ კომპანიის ტელეფონზე დარეკვით და თქვენი SIM-ბარათის შეცვლით. როცა მზად იქნებით, დაიწყოთ 2FA-ს ამოქმედება თქვენი ორგანიზაციის ყველა ანგარიშზე, გამოიყენეთ ვებსაიტი (https://2fa.directory/), რომ სწრაფად გაეცნოთ ინფორმაციას და მითითებებს სპეციფიკური სერვისების (როგორიცაა Gmail, Office 365, Facebook, Twitter და სხვა) შესახებ და გაარკვიოთ, რომელი მათგანი 2FA-ს რომელ ტიპს გაწვდით.

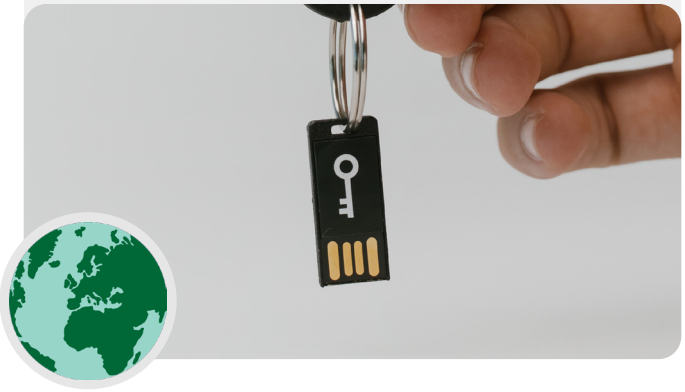
2FA და სამოქალაქო საზოგადოება

Amnesty International-ის ბოლო ანგარიშის თანახმად, ადამიანის უფლებების უზბეკ დამცველებზე შეტევის განმახორციელებელმა ჰაკერებმა გამოიყენეს ფიშინგური შეტევები მათი ელფოსტის ანგარიშების პაროლების *და* ორფაქტორიანი ავთენტიკაციის კოდების მოტყუებით გაზიარების მიზნით Gmail-ის სისტემაში შესვლის ყალბი გვერდების გამოყენებით. ასეთი შეტევები სულ უფრო გახშირდა ორფაქტორიანი ავთენტიკაციისთვის „გვერდის ასავლელად“. მნიშვნელოვანია – 2FA-ს დაყენების შემთხვევაშიც კი ყურადღება მიაქციეთ, სად შეგყავთ კოდები. უფრო უკეთესია, თუ აღმოფხვრით ამ რისკს ფიზიკური უსაფრთხოების გასაღებებით.



დამცავი გასაღებები რეალურ სამყაროში

აუთენტურობის ორფაქტორული შემოწმებისათვის ფიზიკური უსაფრთხოების გასაღებების უზრუნველყოფით 85000-ზე მეტი საკუთარი თანამშრომლისათვის, Google (მეტად მაღალი რისკი, მეტად სასურველი სამიზნე) ეფექტურად აღმოფხვრა ნებისმიერი წარმატებული ფიშინგური შეტევა ორგანიზაციაზე. ხსენებული მაგალითი გვიჩვენებს როგორი ეფექტური შეიძლება იყოს დამცავი გასაღებები მაღალი რისკის ორგანიზაციებისათვისაც კი.



რა ხდება, თუ ვინმე დაკარგავს 2FA-ს მოწყობილობას?

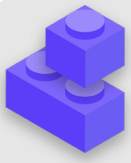
დამცავ გასაღებს მოეპყარით როგორც თქვენი სახლის ან ბინის გასაღებს. ერთი სიტყვით, არ დაკარგოთ ის. როგორც თქვენი სახლის გასაღების შემთხვევაში მუდამ კარგი აზრია, იქონიოთ თქვენს ანგარიშზე რეგისტრირებული სათადარიგო გასაღები, რომელსაც შეინახავთ ჩაკეტილ დაცულ ადგილას (მაგალითად, სახლის ან სადეპოზიტო ყუთის სეიფში) უბრალოდ დაკარგვის ან ქურდობის შემთხვევისათვის. ალტერნატივის სახით, უნდა შექმნათ სათადარიგო კოდები პროფილებისათვის, რომლებიც იძლევა ამის საშუალება. ხსენებული კოდები უნდა შეინახოთ მეტად უსაფრთხო ადგილას, როგორც თქვენი პაროლების დისპეტჩერი ან ფიზიკური სეიფი. აღნიშნული სათადარიგო კოდები, შესაძლოა, დაგენერირდეს თითქმის ყველა საიტის 2FA-ს პარამეტრებით (იქვე, სადაც თავდაპირველად გააქტიურეთ 2FA) და, შესაძლოა, შეასრულოს სათადარიგო გასაღების ფუნქცია აუცილებლობის შემთხვევაში. 2FA-სთან დაკავშირებით ყველაზე გავრცელებული შემთხვევაა, როცა ხალხი ცვლის ან კარგავს ტელეფონს, რომელსაც იყენებდა ავთენტიკაციის აპლიკაციებისათვის. Google Authenticator-ის შემთხვევაში სამწუხაროდ, არ გაგიმართლებთ, თუ ტელეფონს მოგპარავენ და თქვენ არ ინახავდით სარეზერვო კოდებს, რომლებიც გენერირდება Google Authenticator-თან ანგარიშის დაკავშირებისას. ამდენად, თუ Google Authenticator-ს იყენებთ, როგორც 2FA-ს აპლიკაციას, თქვენი ანგარიშების კოდების სარეზერვო ასლი აუცილებლად შეინახეთ დაცულ ადგილას. თუ იყენებთ Authy-ს ან Duo-ს, ორივე აპლიკაციაში არის ჩაშენებული სარეზერვო ასლის შექმნის ფუნქცია უსაფრთხოების მკაცრი პარამეტრებით, რომლებიც შეგიძლიათ, აამოქმედოთ. თუ აირჩევთ ხსენებული აპლიკაციებიდან რომელიმეს, შეგიძლიათ, დააყენოთ სარეზერვო აღრიცხვის ფუნქცია მოწყობილობის გატეხის, დაკარგვის ან ქურდობის შემთხვევისთვის. იხ. ავტორის მითითებები აქ, ხოლო Duo-ს - აქ. უზრუნველყავით, რომ თქვენს ორგანიზაციაში ყველა იყოს ინფორმირებული აღნიშნული ნაბიჯების თაობაზე, როცა დაიწყებენ 2FA-ს ამოქმედებას საკუთარ ანგარიშებზე.



2FA-ს დანერგვა მთელს თქვენს ორგანიზაციაში

თუ თქვენი ორგანიზაცია უქმნის ელფოსტის ანგარიშებს ყველა თანამშრომელს Google Workspace-ის (წარსულში GSuite) ან Microsoft 365-ის მეშვეობით და საკუთარი დომენის (მაგალითად, @ndi.org) გამოყენებით, შეგიძლიათ, დანერგოთ 2FA და უსაფრთხოების მკაცრი პარამეტრები ყველა ანგარიშისთვის.აღნიშნული დაგეხმარებათ არა მხოლოდ ხსენებული ანგარიშების დაცვაში, არამედ ის ასევე გააცნობს 2FA-ს თქვენს პერსონალს ისე, რომ მისი გამოყენება უფრო მოხერხებული იყოს მათთვის პირად ანგარიშებთან მიმართებაშიც.როგორც Google Workspace-ის ადმინისტრატორს, შეგიძლიათ, შეასრულოთ ეს მითითებები თქვენს დომენზე 2FA-ს გამოსაყენებლად.როგორც დომენის ადმინს, მსგავსად შეგიძლიათ, Microsoft 365-შიც გააკეთოთ ამ ნაბიჯების გადადგმით.

ასევე იფიქრეთ თქვენი ორგანიზაციის ანგარიშების „გაუმჯობესებული დაცვის „პროგრამაში“ (Google) ან AccountGuard-ში (Microsoft) ჩართვაზე, რომ დანერგოთ უსაფრთხოების მართვის დამატებითი მექანიზმები და მოითხოვოთ ფიზიკური უსაფრთხოების გასაღებები ორფაქტორიანი ავთენტიკაციისთვის.



პროფილების დაცულობის უზრუნველყოფა

- **მოითხოვეთ ძლიერი პაროლები ყველა ორგანიზაციული პროფილისათვის; წაახალისეთ პერსონალი და მოხალისეები გააკეთონ იგივე პირად პროფილებთან მიმართებაში.**
- **დანერგეთ სანდო პაროლების დისპეტჩერი ორგანიზაციაში (და მოუწოდეთ მისი გამოყენებისკენ პერსონალს პირად ცხოვრებაშიც).**
  - მოითხოვეთ ძლიერი პირველადი პაროლი და 2FA-ი პაროლების დისპეტჩერი ყველა პროფილისათვის.
  - შეახსენეთ ყველას გამოვიდნენ პაროლების დისპეტჩერის სისტემიდან გაზიარებულ მოწყობილობაზე ან როცა მაღალია მოწყობილობის ქურდობის ან კონფისკაციის რისკი.
- **შეცვალეთ გაზიარებული პაროლები ორგანიზაციიდან პერსონალის წასვლისას.**
- **გააზიარეთ პაროლები მხოლოდ უსაფრთხოდ, მაგალითად, თქვენი ორგანიზაციის პაროლების დისპეტჩერის საშუალებით ან აბონენტთაშორისი დაშიფვრის მქონე აპებით.**
- **მოითხოვეთ 2FA-ი ყველა ორგანიზაციულ პროფილზე და წაახალისეთ პერსონალი გამართოს 2Fa-ი ყველა პირად პროფილზეც.**
  - თუ შესაძლებელია, გადაეცით მთელს პერსონალს ფიზიკური უსაფრთხოების გასაღებები.
  - თუ დამცავი გასაღებები არაა გათვალისწინებული თქვენს ბიუჯეტში, წაახალისეთ აუთენტურობის აპების გამოყენება SMS-ის ან ტელეფონით 2FA-ის გაცემის ნაცვლად.
- **გამართეთ რეგულარული ტრენინგი, რათა უზრუნველყოთ პერსონალის ინფორმირება პაროლების და 2FA-ის აღიარებული პრაქტიკის შესახებ, მათ შორის, თუ რა აძლიერებს პაროლს და რატომაა მნიშვნელოვანი პაროლების ხელახლა არასდროს გამოყენება, 2FA-ის მხოლოდ ლეგიტიმური მოთხოვნების მიღება და 2FA-ის სათადარიგო კოდების გენერირება.**

მოწყობილობების დაცვა

გარდა პროფილებისა, ასევე მნიშვნელოვანია ყველა მოწყობილობა – კომპიუტერები, ტელეფონები, USB-ები, გარე მყარი დისკები და სხვა – იყოს კარგად დაცული.

აღნიშნული დაცვა იწყება ყურადღებით იმის მიმართ, თუ რა ტიპის მოწყობილობებს ყიდულობს და იყენებს თქვენი ორგანიზაცია და პერსონალი. თქვენს მიერ არჩეულ ნებისმიერ მომწოდებელს ან მწარმოებელს უნდა გააჩნდეს მოწყობილობის (მაგალითად, ტელეფონების და კომპიუტერების) მიმართ გლობალური სტანდარტების დაცვის დადასტურებული რეპუტაცია. თქვენს მიერ შესყიდული ნებისმიერი მოწყობილობა დამზადებული უნდა იყოს სანდო კომპანიის მიერ, რომელსაც არა აქვს სტიმული გადასცეს მონაცემები და ინფორმაცია პოტენციურ მეტოქეს.

მნიშვნელოვანია აღინიშნოს, რომ ჩინეთის მთავრობა მოითხოვს ჩინური კომპანიებისაგან მიაწოდონ მონაცემები ცენტრალურ ხელისუფლებას. ამდენად, მიუხედავად Huawei-ის ან ZTE-ის სმარტფონების გავრცელების და სიიაფისა, მოერიდეთ მათ. მიუხედავად იმისა, რომ იაფი აპარატურის ფასი შესაძლოა მიმზიდველი იყოს ორგანიზაციისათვის, დემოკრატიის, ადამიანის უფლებების თუ ანგარიშვალდებულების მხარდამჭერი ორგანიზაციების უსაფრთხოების პოტენციურმა რისკებმა უნდა გიბიძგოთ სხვა არჩევანისაკენ, რამდენადაც ხსენებული წვდომა მონაცემებზე დაეხმარა ჩინეთის მთავრობას და სხვა მთავრობებს მიზანში ამოეღოთ კონკრეტული ადამიანები და საზოგადოებები. თქვენმა მეტოქეებმა შესაძლოა ხელყონ თქვენი მოწყობილობების - და ყველაფრის, რასაც ამ მოწყობილობებიდან აკეთებთ - უსაფრთხოება თქვენს აპარატებზე ფიზიკური წვდომის ან „დისტანციური“ წვდომის მიღების საშუალებით.



მოწყობილობის უსაფრთხოება და სამოქალაქო საზოგადოება

მსოფლიოში ყველაზე უფრო თანამედროვე ზოგიერთი საზიანო პროგრამა შეიქმნა და გავრცელდა სამოქალაქო საზოგადოებრივი ორგანიზაციების და ადამიანის უფლებების დამცველთა მიზანში ამოსაღებად. ინდოეთში, მაგალითად, Amnesty International-ის [ცნობით](), 2020 წელს ადამიანის უფლებების, სულ მცირე, ცხრა დამცველის მობილური აპარატები და კომპიუტერები შეიქნა სათვალთვალო პროგრამის (საზიანო პროგრამული უზრუნველყოფის ტიპი) მსხვერპლი. სათვალთვალო პროგრამა ინერგებოდა არაერთი ფიშინგ ელ-შეტყობინების საშუალებით, რომლებიც შეიცავდა ბმულებს Firefox Send-ით (დღემდე გაუუქმებელი ფაილების გაზიარების პროგრამა) გაზიარებულ ინფიცირებულ ფაილებზე. იმ მსხვერპლის მოწყობილობები, რომლებმაც გახსნეს ფაილები, დავირუსდა პროგრამული უზრუნველყოფით, რომელიც იწერდა აუდიოს, აღრიცხავდა კლავიატურაზე მუშაობას და შეტყობინებებს და ფაქტიურად აქცევდა მათ თავდამსხმელების მიერ თვალთვალის ობიექტებად. შეტევები, რომლებიც ხშირად ისახავს მიზნად სამოქალაქო საზოგადოების ჯგუფებს და მათ ინდივიდუალურ წევრებს, სამწუხაროდ წარმოადგენს შემტევების ჩვეულ მეთოდს მიიღონ „დისტანციური“ წვდომა მოწყობილობაზე.



მოწყობილობაზე ფიზიკური წვდომა დაკარგვის ან ქურდობის შედეგად

ფიზიკურ ხელყოფის პრევენციისათვის, მნიშვნელოვანია ფიზიკურად დაცულ ადგილას შეინახოთ თქვენი მოწყობილობები. ერთი სიტყვით, ნუ გაუმარტივებთ მეტოქეს თქვენი მოწყობილობის ქურდობას ან დროებით მიღებასაც კი. შეინახეთ მოწყობილობები ჩაკეტილ ადგილას, თუ ტოვებთ მათ სახლში ან სამსახურში. ან თუ თვლით, რომ უფრო უსაფრთხოა, იქონიეთ ისინი თან. რა თქმა უნდა, აღნიშნული ნიშნავს, რომ მოწყობილობის უსაფრთხოების ნაწილი მოიცავს თქვენი სამუშაო ადგილის (როგორც სამსახურში, ისე სახლში) უსაფრთხოებას. თქვენ უნდა დააყენოთ საიმედო საკეტები, უსაფრთხოების კამერები ან სხვა მონიტორინგის სისტემები - განსაკუთრებით, თუ თქვენი ორგანიზაცია მაღალ რისკს განიცდის. შეახსენეთ პერსონალს ისევე მიუდგეს მოწყობილობებს, როგორც მიუდგებოდა დიდი ოდენობით ფულს - არ დატოვოს ისინი უყურადღებოდ ან დაუცველი.

რა ხდება, თუ მოწყობილობას მოიპარავენ?

თუ ვინმე მოახერხებს მოწყობილობის მოპარვას - ან თუ ის მიიღებს წვდომას დროის მცირე პერიოდითაც კი – ზიანის შესამცირებლად, უზრუნველყავით რომ **სავალდებულო იყოს ძლიერი პაროლის ან კოდის გამოყენება ყველას კომპიუტერზე ან ტელეფონზე.** კომპიუტერის თუ ლეპტოპის კარგ პაროლზეც ვრცელდება იგივე რეკომენდაციები, რომლებიც მოცემულია წინამდებარე სახელმძღვანელოს პაროლების სექციაში. რაც შეეხება თქვენი ტელეფონის ბლოკირებას, გამოიყენეთ კოდი, რომელიც მოიცავს, სულ მცირე, ექვსიდან რვა ციფრამდე და მოერიდეთ ეკრანის განსაბლოკად „გასმითი კომბინაციების“ გამოყენებას. დამატებითი რეკომენდაციები ეკრანის ბლოკირების შესახებ იხ. Tactical Tech-ის **Data Detox Kit**. მოწყობილობის კარგი პაროლების გამოყენება გაცილებით ურთულებს მეტოქეს სწრაფად მოიპოვოს წვდომა ინფორმაციაზე თქვენს მოწყობილობაში ქურდობის ან კონფისკაციის შემთხვევაში. რთული კოდის დაყენების შემთხვევაში, საკმარისია სახით ან თითის ანაბეჭდით განბლოკვის აქტივაცია, თუმცა, დარწმუნდით, რომ გამორთეთ ის (რთული კოდის გამორთვის გარეშე) რაიმე რისკის მომცველის (მაგალითად, საპროტესტო აქცია ან საზღვრის გადაკვეთა) დაწყებამდე, თუ თქვენ და თქვენი პერსონალი შეშფოთებული ხართ მოწყობილობის ორგანოების მიერ კონფისკაციის გამო. თუ ორგანიზაციის მიერ გაცემულ რომელიმე მოწყობილობას გააჩნია „იპოვე ჩემი მოწყობილობის“ ფუნქცია, როგორიცაა iPhone-ის Find My iPhone და Android-ის Find My Device, განიხილეთ პერსონალისაგან მისი აქტივაციის მოთხოვნა. წაახალისეთ პერსონალი გამოიყენოს ფუნქციები პირად მოწყობილობებზეც. ამ ფუნქციების ჩართვის შემთხვევაში აპარატის მესაკუთრეს (ან მინდობილ პირს) შეუძლია, დაადგინოს მოწყობილობის ლოკაცია ან დისტანციურად წაშალოს მისი შიგთავსი ქურდობის, დაკარგვის ან კონფისკაციის შემთხვევაში. iPhone-ების შემთხვევაში, ასევე შეგიძლიათ მოახდინოთ მოწყობილობის კონფიგურაცია ისე, რომ ავტომატურად წაშალოს ყველაფერი სისტემაში შესვლის რამდენიმე წარუმატებელი მცდელობის შემდეგ. მოწყობილობის მართვის აღნიშნული ფუნქციები გადამწყვეტ მნიშვნელობას იძენს, თუ სენსიტიური ინფორმაციის შემცველი მოწყობილობა დაიკარგა ან მოხვდა უცხო ხელში.

რას იტყვით მოწყობილობის დაშიფვრაზე?

მნიშვნელოვანია ყველა მოწყობილობაში, განსაკუთრებით კომპიუტერებში და სმარტფონებში, გამოვიყენოთ მონაცემთა დაშიფვრა, სკრემბლინგი ისე, რომ ის შეიქნას არაკითხვადი და უსარგებლო. თუ შესაძლებელია, თქვენი ორგანიზაციის ყველა მოწყობილობა უნდა აღჭურვოთ უნარით, რომელსაც **დისკის სრულად დაშიფვრა** ეწოდება. დისკის სრულად დაშიფვრა გულისხმობს, რომ მოწყობილობის მთელი დისკი დაშიფრულია ისე, რომ, თუ ქურდობის საგნად იქცევა, არ შეეძლებათ, ამოიღონ მოწყობილობის შიგთავსი პაროლის ან დასაშიფრად გამოყენებული გასაღების ცოდნის გარეშე. დისკის სრულად დაშიფვრას არაერთი თანამედროვე სმარტფონი და კომპიუტერი გვთავაზობს. Apple-ის მოწყობილობები, როგორიცაა iPhone-ები და iPad-ები, საკმაოდ მოსახერხებლად რთავს დისკის სრულად დაშიფვრას, როცა აყენებთ მოწყობილობის ჩვეულებრივ კოდს. Apple-ის კომპიუტერები, რომლებიც გამოიყენებს macOS-ს, გთავაზობს ფუნქციას, რომელსაც FileVault ეწოდება, რომელიც შეგიძლიათ ჩართოთ დისკის სრულად დაშიფვრისათვის. Windows-ის კომპიუტერები, რომლებიც ამუშავებს პრო-, საწარმო ან საგანმანათლებლო ლიცენზიას, გვთავაზობს ფუნქციას BitLocker, რომელიც შეგიძლიათ, ჩართოთ დისკის სრულად დაშიფვრისათვის. შეგიძლიათ, ჩართოთ BitLocker Microsoft-ის **ამ მითითებების** შესრულებით, რომელიც შესაძლოა ჯერ ასამოქმედებელი იყოს თქვენი ორგანიზაციის ადმინისტრატორის მიერ. თუ პერსონალს აქვს მხოლოდ სახლის ლიცენზია საკუთარი Windows-ის კომპიუტერებისათვის, BitLocker არ არის ხელმისაწვდომი. თუმცა, მათ შეუძლიათ ჩართონ დისკის სრულად დაშიფვრა Windows OS-ის პარამეტრებში ‘Update & Security’ > ‘Device encryption’-დან.

Android-ის აპარატებს, 9.0 და უფრო გვიანი ვერსიებიდან, გააჩნია ფაილების საფუძველზე დაშიფვრა, ჩართული უპირობოდ. Android-ის ფაილების საფუძველზე დაშიფვრის მუშაობა განსხვავდება დისკის სრულად დაშიფვრისაგან, თუმცა, მაინც უზრუნველყოფს მაღალი დონის უსფრთხოებას. თუ იყენებთ Android-ის შედარებით ახალ ტელეფონს და დაყენებული გაქვთ კოდი, გააქტიურებული უნდა იყოს ფაილების საფუძველზე დაშიფვრაც. თუმცა, კარგი აზრია შეამოწმოთ თქვენი პარამეტრები უბრალოდ რომ დარწმუნდეთ, განსაკუთრებით, თუ თქვენი ტელეფონი რამდენიმე წელიწადზე მეტისაა. შესამოწმებლად გადადით თქვენი Android-ის აპარატის to Settings > Security-ში. უსაფრთხოების პარამეტრებში ნახავთ ქვესექციას „encryption“ ან „encryption and credentials“, რომელიც გიჩვენებთ, არის თქვენი ტელეფონი დაშიფრული თუ არა და თუ არ არის, შეგიძლიათ, ჩართოთ დაშიფვრა.

კომპიუტერების (როგორც Windows-ის, ისე Mac-ის) შემთხვევაში, კონკრეტულად მნიშვნელოვანია, უსაფრთხო ადგილას შეინახოთ დაშიფვრის ნებისმიერი გასაღები (ასევე ცნობილია, როგორც აღდგენის გასაღები). ხსენებული „აღდგენის გასაღებები“, უმეტეს შემთხვევაში, წარმოადგენს გრძელ პაროლებს ან კოდურ ფრაზებს. თუ დაგავიწყდათ თქვენი მოწყობილობის პაროლი ან მოხდა რაიმე მოულოდნელი (მაგალითად, მოწყობილობის მწყობრიდან გამოსვლა), აღდგენის გასაღებები წარმოადგენს ერთადერთ გზას დაშიფრული მონაცემების აღსადგენად და, საჭიროების შემთხვევაში, მათ ახალ მოწყობილობაში გადასაწერად. ამდენად, დისკის სრულად დაშიფვრის გამორთვისას აუცილებლად შეინახეთ ხსენებული გასაღებები თუ პაროლები უსაფრთხო ადგილას, როგორიცაა უსაფრთხო დისტანციური ანგარიში ან თქვენი ორგანიზაციის პაროლების მენეჯერი.

მოწყობილობაზე დისტანციური წვდომა – ასევე ცნობილია, როგორც ჰაკინგი

გარდა მოწყობილობის ფიზიკურად უსაფრთხოდ შენახვისა, მნიშვნელოვანია, დავიცვათ ისინი საზიანო პროგრამისაგან. Tactical Tech-ის **Security-in-a-Box-ში** მოცემულია სასარგებლო აღწერა იმისა, თუ რა არის საზიანო პროგრამა და რატომაა მნიშვნელოვანი მისთვის თავის არიდება, რაც მარტივად ასახულია მოცემული სექციის დანართჩენ ნაწილში.

საზიანო პროგრამის ინტერპრეტაცია და თავიდან აცილება

არსებობს საზიანო პროგრამის (რომელიც, განსაზღვრების თვალსაზრისით, წარმოადგენს საზიანო პროგრამულ უზრუნველყოფას) კლასიფიკაციის არაერთი გზა. ჭია-ვირუსები ვირუსები, ჯაშუშური პროგრამები, ჭიები, ტროიანები, რუტკიტები, გამომძალველი პროგრამები და კრიპტოჯეკერები წარმოადგენს მავნე პროგრამულ უზრუნველყოფას. ზოგიერთი საზიანო პროგრამულ უზრუნველყოფა ვრცელდება ინტერნეტში ელ-ფოსტის, ტექსტური შეტყობინებების, საზიანო ვებგვერდების და სხვა საშუალებებით. ზოგიერთი ვრცელდება მოწყობილობებით, როგორიცაა USB-ის მეხსიერების ჩიპები, რომლებიც გამოიყენება მონაცემთა გაზიარების და ქურდობის მიზნით. და როცა ზოგიერთი საზიანო პროგრამული უზრუნველყოფა საჭიროებს მიმნდობი სამიზნის მიერ შეცდომის დაშვებას, სხვებს შეუძლიათ ჩუმად მოახდინოს მოწყვლადი სისტემების ინფიცირება თქვენ მიერ რაიმე არასწორი ქმედების გარეშეც.

გარდა ზოგადი საზიანო პროგრამული უზრუნველყოფისა, რომელიც ვრცელდება ყველგან და მიმართულია სამოქალაქო საზოგადოებაზე, მიზნობრივი საზიანო პროგრამული უზრუნველყოფა, ჩვეულებრივ, გამოიყენება კონკრეტული პიროვნების, ორგანიზაციის ან ქსელის შეფერხების ან მასზე თვალთვალისათვის. აღნიშნულ მეთოდიკას იყენებენ ჩვეულებრივი კრიმინალები, თუმცა, ასევე იქცევიან სამხედრო და სადაზვერვო სამსახურებიც, ტერორისტები, ონლაინ შემწუხებლები, მეუღლეები შემავიწროვებელი ქცევით და საეჭვო პოლიტიკური მოღვაწეები.

თუმცა, რაც არ უნდა იყოს მათი სახელი, და გავრცელების გზები, საზიანო პროგრამულ უზრუნველყოფას შეუძლია, გაანადგუროს კომპიუტერები, მოიპაროს და გაანადგუროს მონაცემები, გააკოტროს ორგანიზაციები, ხელყოს კონფიდენციალურობა და საფრთხე შეუქმნას მომხმარებლებს. ერთი სიტყვით, საზიანო პროგრამული უზრუნველყოფა მართლაც სახიფათოა. თუმცა, არსებობს რამდენიმე მარტივი ნაბიჯი, რომლებიც შეუძლია, გადადგას თქვენს ორგანიზაციას ხსენებული საყოველთაო საფრთხისაგან თავის დასაცავად.

დაგვიცავს ანტი-საზიანო პროგრამული უზრუნველყოფა?

ანტი-საზიანო პროგრამული უზრუნველყოფა, სამწუხაროდ, არაა სრულად გადაწყვეტა. თუმცა, მეტად კარგი აზრია თავიდან გამოიყენოთ ზოგიერთი საბაზისო უფასო ინსტრუმენტი. საზიანო პროგრამული უზრუნველყოფა იმდენად სწრაფად იცვლება და იმდენად ხშირად იძენს ახალ რისკებს რეალურ სამყაროში, რომ რომელიმე ასეთ ინსტრუმენტზე დაყრდნობა ვერ იქნება დაცვის თქვენი ერთადერთი საშუალება.

თუ იყენებთ Windows-ს, უნდა გაცნობოდით Windows-ის ჩაშენებულ Defender-ს. Mac-ები და Linux-ის კომპიუტერები და არც Android-ის და iOS-ის მოწყობილობები არ ფუნქციონირებს ჩაშენებული ანტი-საზიანო პროგრამული უზრუნველყოფით. ამ მოწყობილობებზე (და Windows-ის კომპიუტერებზეც) შეგიძლიათ, დააყენოთ სანდო და უფასო ხელსაწყო, როგორიცაა **Bitdefender** ან **Malwarebytes**. **თუმცა, ნუ დაეყრდნობით მათ, როგორც დაცვის ერთადერთ საშუალებას,** რადგან ისინი რა თქმა უნდა გაუშვებენ ზოგიერთ მაქსიმალურად მიზნობრივ და სახიფათო ახალ შეტევებს.

გარდა ამისა, მეტად ყურადღებით იყავით, რომ ჩამოტვირთოთ მხოლოდ აღიარებული ანტი-საზიანო პროგრამული უზრუნველყოფა ან ანტი-ვირუსები ლეგიტიმური წყაროებიდან (როგორიცაა ზემოთ მოცემული ვებგვერდების ბმულები). სამწუხაროდ, არსებობს ანტი-საზიანო პროგრამული უზრუნველყოფის არაერთი ყალბი თუ გატეხილი ვერსია, რომლებიც კარგზე მეტ ცუდს აკეთებენ.

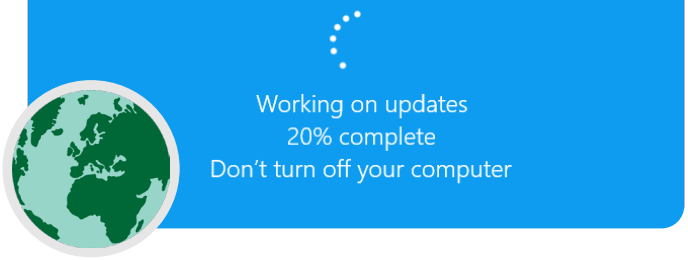
თუ თქვენს ორგანიზაციაში Bitdefender-ს ან საზიანო პროგრამების საწინააღმდეგო სხვა ხელსაწყოს იყენებთ, ორი მათგანი ერთდროულად არ უნდა ჩართოთ. არაერთი მათგანი აღიქვამს მეორე ანტი-საზიანო პროგრამული უზრუნველყოფის ქცევას საეჭვოდ და აჩერებს მის მუშაობას რაც იწვევს ორივეს გაუმართაობას. Bitdefender ან საზიანო პროგრამების საწინააღმდეგო სხვა სანდო ხელსაწყოები უფასოდ შეიძლება განახლდეს, ხოლო ჩაშენებული Windows Defender განახლებებს თქვენს კომპიუტერთან ერთად იღებს. უზრუნველყავით, რომ თქვენმა ანტი-საზიანო პროგრამულმა უზრუნველყოფამ რეგულარულად თავად განაახლოს თავი (კომერციული პროგრამული უზრუნველყოფის ზოგიერთი საცდელი ვერსია, რომელიც მიეწოდება კომპიუტერთან ერთად, დეაქტივირდება საცდელი ვადის გასვლის შემდეგ, რაც უფრო სახიფათოა, ვიდრე სასარგებლო). ახალი საზიანო პროგრამული უზრუნველყოფა იწერება და ვრცელდება ყოველდღიურად, ამიტომ, თქვენი კომპიუტერი სწრაფად შეიქნება უფრო მოწყვლადი, თუ თვალს არ მიადევნებთ ახალ საზიანო პროგრამულ უზრუნველყოფას და ანტი-საზიანო პროგრამული უზრუნველყოფის მეთოდიკას. თუ შესაძლებელია, თქვენი პროგრამული უზრუნველყოფის კონფიგურაცია ისე უნდა მოახდინოთ, რომ განახლებების ინსტალაცია იყოს ავტომატური. თუ თქვენს ანტი-საზიანო პროგრამულ უზრუნველყოფას გააჩნია ფუნქცია „მუდამ ჩართული“, უნდა აამოქმედოთ ის და აწარმოოთ თქვენს კომპიუტერში დაცული ფაილების პერიოდული სკანირება.

იქონიეთ მოწყობილობები განახლებულ მდგომარეობაში

განახლება უმნიშვნელოვანესია. გამოიყენეთ მოწყობილობაში მომუშავე ნებისმიერი ოპერაციული სისტემის ბოლო ვერსია (Windows, Mac, Android, iOS და სხვა) და იქონიეთ ხსენებული ოპერაციული სისტემა განახლებულ მდგომარეობაში. ასევე მუდამ განახლებულ მდგომარეობაში იქონიეთ სხვა პროგრამული უზრუნველყოფა, ბრაუზერი და მისი ნებისმიერი მიერთებული მოდული. დააინსტალირეთ განახლებები მაშინვე, როცა ის შეიქნება ხელმისაწვდომი, იდეალურ შემთხვევაში, **ავტომატური განახლების ამოქმედებით.** რაც უფრო თანამედროვეა მოწყობილობის ოპერაციული სისტემის ვერსია, მით ნაკლებად მოწყვლადი ხართ თქვენ. იფიქრეთ განახლებებზე, როგორც ღია ჭრილობაზე პლასტირის დადებაზე: ის აღმოფხვრის მოწყვლადობას და მნიშვნელოვნად ამცირებს შესაძლებლობას, რომ იქნეთ ინფიცირებული. ასევე, აწარმოეთ იმ პროგრამული უზრუნველყოფის დეინსტალაცია, რომელსაც აღარ იყენებთ. მოძველებულ პროგრამულ უზრუნველყოფას ხშირად უჩნდება უსაფრთხოების პრობლემები, თქვენ კი შესაძლოა დაყენებული გქონდეთ ინსტრუმენტი, რომელიც აღარ განახლდება შემქმნელის მიერ და უფრო მოწყვლადია ჰაკერებისათვის.

საზიანო პროგრამული უზრუნველყოფა რეალურ სამყაროში: განახლება უმნიშვნელოვანესია

2017 წელს გამომძალველი პროგრამა WannaCry თავს დაესხა მილიონობით ინფიცირებულ მოწყობილობას მთელს მსოფლიოში და მოახდინა საავადმყოფოების, სამთავრობო უწყებების, დიდი და მცირე ორგანიზაციების და ბიზნესების ბლოკირება ათობით ქვეყანაში. რატომ იყო შეტევა ამდენად ეფექტური? მოძველებული, „გაუმართავი“ Windows-ის ოპერაციული სისტემების გამო, რომელთაგან არაერთი თავიდანვე გატეხილი იყო. ზიანის დიდი ნაწილი – ადამიანური და ფინანსური – შესაძლოა თავიდან ყოფილიყო აცილებული განახლების უკეთესი ავტომატური მეთოდიკით და ლეგიტიმური ოპერაციული სისტემების გამოყენებით.



ფრთხილად იყავით USB-ებთან

იყავით ყურადღებით იმ ფაილების გახსნისას, რომლებიც გამოგზავნილია დანართით, ჩამოტვირთვის ბმულით ან ნებისმიერი სხვა სახით. ასევე, **ორჯერ დაფიქრდით USB-ის ჩიპების მსგავსი მოძრავი or გადაადგილებადი მატარებლების**, მეხსიერების ფლეშ-ბარათების, DVD-ების და Cd-ების თქვენს კომპიუტერში ჩართვამდე, რადგან ისინი შესაძლოა საზიანო პროგრამული უზრუნველყოფის გადამტანი იყოს. USB-ები, რომლებიც გაზიარებული იყო გარკვეული დროით, მეტად სავარაუდოა იყოს დავირუსებული. თქვენს ორგანიზაციაში ფაილების უსაფრთხოდ გაზიარების ალტერნატიული შესაძლებლობები იხ. „სახელმძღვანელოს“ ფაილების გაზიარების სექცია.

ასევე იყავით ყურადღებით ბლუთუზით დაკავშირებულ სხვა მოწყობილობებთან მიმართებაში. კარგია თქვენი ტელეფონის ან კომპიუტერის სინქრონიზაცია ცნობილ და სანდო ბლუთუზ-სპიკერთან თქვენი საყვარელი მუსიკის მოსასმენად, მაგრამ იყავით ფრთხილად იმ მოწყობილობასთან შეერთებისას, რომელსაც არ იცნობთ. დაუშვით შეერთება მხოლოდ სანდო მოწყობილობებთან და არ დაგავიწყდეთ ბლუთუზის გამორთვა, როცა აღარ იყენებთ მას.

ბრაუზინგისას მოიქეცით გონივრულად

არასდროს დაუშვათ და გაუშვათ პროგრამები, რომლებიც მოდის ვებგვერდებიდან, რომლებსაც არ იცნობთ და ენდობით. მაგალითად, ბრაუზერის ჩამოსაშლელი ფანჯრიდან შემოთავაზებული „განახლების“ დაშვებამდე შეამოწმეთ განახლებები შესაბამისი აპლიკაციის ოფიციალურ ვებგვერდზე. თანახმად „სახელმძღვანელოს“ ფიშინგის სექციაში განხილულისა, მნიშვნელოვანია ვიყოთ ფრთხილად ვებგვერდებზე ბრაუზინგისას. მასზე დაწკაპუნებამდე შეამოწმეთ ბმულის მდებარეობა (მასზე მაუსის მიტანით) და დახედეთ ვებგვერდის მისამართს ბმულზე გადასვლის შემდეგ, რათა დარწმუნდეთ, რომ ის შესაფერისად გამოიყურება სენსიტიური ინფორმაციის, მაგალითად, თქვენი პაროლის შესატანად. ნუ დააწკაპუნებთ შეცდომის შეტყობინებებზე ან გაფრთხილებებზე, უყურეთ ბრაუზერის ფანჯრებს, რომლებიც ავტომატურად ჩნდება და იკითხეთ ისინი ყურადღებით უბრალოდ „Yes“-ზე ან „Ok“-ზე დაწკაპუნების ნაცვლად.

რას იტყვით სმარტფონებზე?

როგორც კომპიუტერების შემთხვევაში, მუდამ განახლებული იქონიეთ თქვენი ტელეფონის ოპერაციული სისტემა და აპლიკაციები და ჩართეთ ავტომატური განახლება. აწარმოეთ ინსტალაცია მხოლოდ ოფიციალური ან სანდო წყაროებიდან, როგორიცაა Google's Play Store-ი და Apple's App Store-ი (ან F-droid-ი, უფასო, ღია კოდის მქონე აპების მაღაზია Android-თვის). აპებში შესაძლოა ჩასმული იყოს საზიანო პროგრამული უზრუნველყოფა და მაინც თითქოს გამართულად მუშაობდეს ისინი, ამიტომ ყოველთვის არ იცით არის თუ არა რომელიმე საზიანო. ასევე უზრუნველყავით, რომ ჩამოტვირთოთ აპლიკაციის ლეგიტიმური ვერსია. ვერიის ჩამოტვირთვას. განსაკუთრებით Android-თვის არსებობს პოპულარული აპლიკაციების „ყალბი“ ვერსიები. ასე, რომ დარწმუნდით, რომ აპი შექმნილი იყოს შესაფერისი კომპანიის ან დეველოპერის მიერ, გააჩნდეს კარგი გამოხმაურება და გააჩნდეს ჩამოტვირთვების მოსალოდნელი რაოდენობა (მაგალითად, WhatsApp-ის ყალბ ვერსიას შესაძლოა ჰქონდეს მხოლოდ რამდენიმე ათასი ჩამოტვირთვა, ხოლო რეალურ ვერსიას ხუთ მილიარდზე მეტი აქვს). ყურადღება მიაქციეთ ნებართვებს, რომლებსაც მოითხოვს თქვენი აპები. თუ ისინი ზედმეტად გამოიყურება (მაგალითად, კალკულატორი ითხოვს წვდომას თქვენს კამერაზე ან Angry Birds-ი ითხოვს წვდომას თქვენს ლოკაციაზე), უარყავით მოთხოვნა ან მოახდინეთ აპის დეინსტალაცია. იმ აპების დეინსტალაცია, რომლებსაც აღარ იყენებთ, შესაძლოა ასევე დაგეხმაროთ თქვენი სმარტფონის თუ ტაბლეტის დაცვაში. ხანდახან დეველოპერები მიჰყიდიან საკუთარ აპებზე საკუთრების უფლებას სხვებს. ეს ახალი მესაკუთრეები შესაძლოა შეეცადონ იშოვონ ფული საზიანო კოდის ჩამატებით.

საზიანო პროგრამული უზრუნველყოფა რეალურ სამყაროში: მობილურის საზიანო აპები

ჰაკერები წლების მანძილზე მრავალ ქვეყანაში იყენებდნენ ყალბ აპლიკაციებს Google Play store-ში საზიანო პროგრამული უზრუნველყოფის გასავრცელებლად. ერთ კონკრეტულ შემთხვევაში, რომელსაც სინათლე 2020 წ. მოეფინა, ის მიმართული იყო ვიეტნამელი მომხმარებლის წინააღმდეგ. თვალთვალის ამ კამპანიაში გამოიყენებოდა ყალბი აპლიკაციები, რომელიც უნდა დახმარებოდა მომხმარებელს ახლომდებარე პაბების ან ადგილობრივი ეკლესიების შესახებ ინფორმაციის მოძიებაში. Android-ის არაინფორმირებული მომხმარებლის მიერ ინსტალაციის შემდეგ საზიანო აპლიკაციები აგროვებდა ზარების ჟურნალებს, ლოკაციის მონაცემებს და ინფორმაციას კონტაქტების და ტექსტური შეტყობინებების შესახებ. ესაა მრავალიდან ერთ მიზეზი იმისა, რომ იყოთ ყურადღებით თქვენს მოწყობილობაში აპლიკაციების ჩამოტვირთვისას.



დაზოგეთ მეტი ფული და აამაღლეთ მოწყობილობის უსაფრთხოება Tails-ის საშუალებით თქვენს ორგანიზაციაში

ერთი მეტად უსაფრთხო ოფცია, რომელიც გასამართად საჭიროებს მცირე ტექნიკურ უნარს, არის Tails-ის ოპერაციული სისტემა. აღნიშნული პორტატული საოპერაციო სისტემა უფასოა გამოსაყენებლად და შეგიძლიათ ჩატვირთოთ პირდაპირ USB-დან Windows-ის ან Mac-ის საოპერაციო სისტემების საჭიროების გვერდის ავლით. Tails-ი ასევე კარგი არჩევანია მაქსიმალური რისკის მქონეთათვის, რადგან ის შეიცავს კონფიდენციალურობის გამაძლიერებელი ფუნქციების ფართო სპექტრს. ხსენებული ფუნქციები მოიცავს Tor-ის (განხილულია ქვემოთ) ინტეგრაციას, რათა უზრუნველყოფილი იქნეს თქვენი ინტერნეტ-ტრაფიკი და მეხსიერების სრულად გასუფთავება ყოველთვის როცა გამორთავთ საოპერაციო სისტემას. აღნიშნული ფუნქციები არსებითად გაძლევთ საშუალებას დაიწყოთ ახალი ფურცლიდან მუდამ, როცა ხელახლა ჩართავთ თქვენს კომპიუტერს. Tails-ს ასევე გააჩნია შენახვის რეჟიმი, რომელიც, სურვილის შემთხვევაში, საშუალებას გაძლევთ შეინახოთ ფაილები და პარამეტრები არაერთი სეანსიდან.

უფასო, უსაფრთხო ოპერაციული სისტემის კიდევ ერთი ოფციაა Qubes OS. მიუხედავად იმისა, რომ არაა მარტივი ოფცია არატექნიკური მომხმარებლისათვის, Qubes-ის მიზანია შეზღუდოს საზიანო პროგრამული უზრუნველყოფის საფრთხე და წარმოადგენს კიდევ ერთ გასათვალისწინებელ ოფციას გამოცდილი და მაღალი რისკის მქონე მომხმარებლისათვის თქვენს ორგანიზაციაში, განსაკუთრებით, თუ ლიცენზირების ფასი პრობლემას წარმოადგენს.

რა ხდება, თუ არ გვაქვს ლეგალური პროგრამული უზრუნველყოფის საშუალება?

პოპულარული პროგრამული უზრუნველყოფის, მაგალითად, Microsoft Office-ის (Word-ი, Powerpoint-ი, Excel-ი) ლიცენზირებული ვერსიების ყიდვა მთელი თქვენი ორგანიზაციისათვის შესაძლოა ძვირი იყოს, თუმცა, შეზღუდული ბიუჯეტი არ ამართლებს პროგრამული უზრუნველყოფის პირატული ვერსიების ჩამოტვირთვას ან მისი მუდმივი განახლების ვერ მოხერხებას. ეს არაა მორალური პრობლემა – ეს უსაფრთხოების საკითხია. პირატული პროგრამული უზრუნველყოფა ხშირად სავსეა საზიანო პროგრამებით და ვერ ავსებს ხვრელებს უსაფრთხოებასი. თუ ვერ ყიდულობთ პროგრამულ უზრუნველყოფას თქვენი ორგანიზაციის საჭირობებისათვის, არსებობს მშვენიერი, უფასო პროგრამული უზრუნველყოფის ფართო არჩევანი, როგორიცაა LibreOffice-ი (სტანდარტული Microsoft Office-ის შემცვლელი აპები) ან GIMP-ი (ფოტოშოფის შემცვლელი), რომლებიც დააკმაყოფილებს თქვენს საჭიროებებს. ასევე იფიქრეთ Tech Soup-ის საშუალებით, ორგანიზაციის, რომელიც სთავაზობს არაკომერციულ ორგანიზაციებს უზარმაზარ ფასდაკლებებს პოპულარულ პროგრამულ უზრუნველყოფაზე. მაშინაც კი, თუ შეგიძლიათ იყიდოთ ლეგიტიმური პროგრამული უზრუნველყოფა და აპები, თქვენი მოწყობილობა მაინც განიცდის რისკს, თუ ლეგიტიმური არაა სერვერის ოპერაციული სისტემა. ამგვარად, თუ თქვენი ორგანიზაცია ვერ ყიდულობს Windows-ის ლიცენზიებს, იფიქრეთ უფრო იაფი ალტერნატივის შესახებ, როგორიცაა Chromebooks-ი, რომელიც მშვენიერი და დაცული ოფციაა, თუ თქვენი ორგანიზაცია უმეტესად ქლაუდით მუშაობს. თუ იყენებთ Google Docs-ს ან Microsoft 365-ს, საერთოდ არ გჭირდებათ ბევრი კომპიუტერული აპლიკაცია - უფასო ბროუზერსშიდა დოკუმენტების და ცხრილების რედაქტორი სრულიად საკმარისია თითქმის ყველა დანიშნულებისთვის. კიდევ ერთი შესაძლებლობა, თუ თქვენს პერსონალს გააჩნია ტექნიკური უნარები, არის Linux-ზე დაფუძნებული უფასო ოპერაციული სისტემის (ღია კოდის მქონე ალტერნატივა Windows-ის და Mac-ის ოპერაციული სისტემებისათვის) ინსტალაცია თითოეულ კომპიუტერზე. ერთი პოპულარული, მეტ-ნაკლებად მომხმარებელზე ორიენტირებული Linux-ის ოფციაა Ubuntu. მიუხედავად იმისა, რომელ საოპერაციო სისტემას აირჩევთ, დარწმუნდით, რომ ვინმე ორგანიზაციაში პასუხისმგებელია პერსონალის ინფორმირებაზე, რათა უზრუნველყოფილი იქნეს, რომ ისინი იყენებენ ბოლო განახლებებს.

ახალი ინსტრუმენტის ან სისტემის თაობაზე გადაწყვეტილების მიღებისას მოიფიქრეთ როგორ შეუძლია თქვენს ორგანიზაციას მისი ტექნიკური და ფინანსური მხარდაჭერა გრძელვადიან პერსპექტივაში. ჰკითხეთ საკუთარ თავს მაგალითად: შეგიძლიათ დაიქირაოთ ან იყოლიოთ პერსონალი ახალი ინსტრუმენტის ან სისტემის უსაფრთხო ექსპლუატაციისთვის? შეგიძლიათ პერიოდული გამოწერების ანაზღაურება? გაქვთ წვდომა ზემოხსენებული Tech Soup-ის მსგავსი ჯგუფების ფასდაკლებებზე? აღნიშნულ კითხვებზე პასუხი შესაძლოა დაგეხმაროთ პროგრამული უზრუნველყოფის და ტექ-სტრატეგიების წარმატებულობის ამაღლების უზრუნველყოფაში დროთა განმავლობაში.



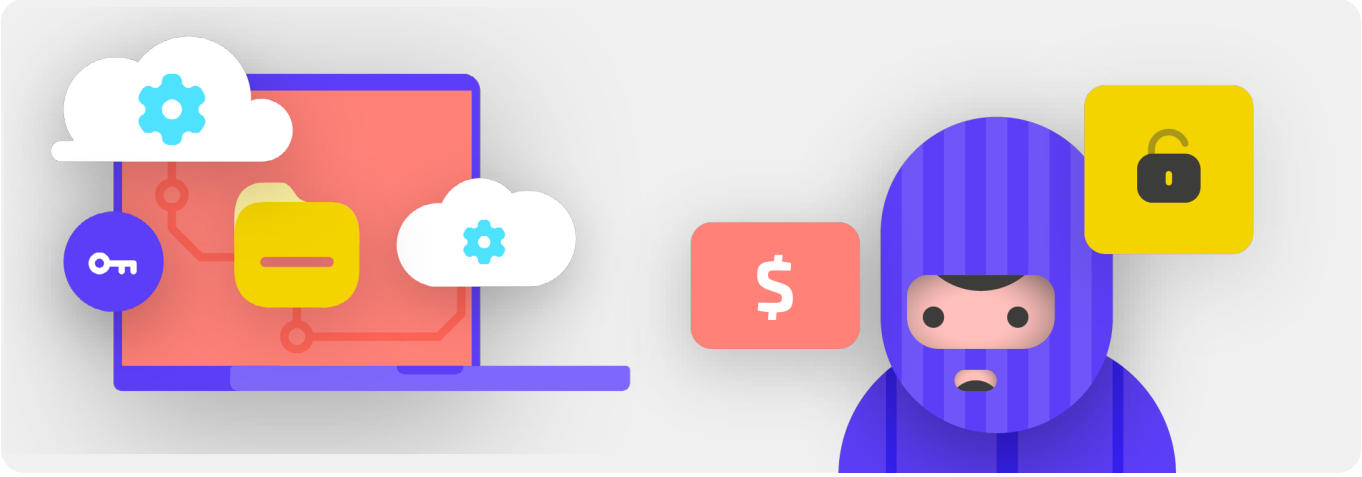
მოწყობილობის უსაფრთხოდ შენახვა

- **აწარმოეთ პერსონალის ტრენინგი საზიანო პროგრამული უზრუნველყოფის რისკების და მისი თავიდან ასაცილებელი აღიარებული პრაქტიკის შესახებ.**
  - შეიმუშავეთ პოლიტიკა გარე მოწყობილობების დაკავშირების, ბმულებზე დაწკაპუნების, ფაილების და აპების ჩამოტვირთვის და პროგრამული უზრუნველყოფის და აპის ნებართვების შემოწმების შესახებ.
- **დააწესეთ, რომ მოწყობილობები, პროგრამული უზრუნველყოფა და აპლიკაციები მუდამ იყოს სრულად განახლებული.**
  - ჩართეთ ავტომატური განახლება, სადაც შესაძლებელია.
- **დარწმუნდით, რომ ყველა მოწყობილობაზე გამოიყენებოდეს ლიცენზირებული პროგრამული უზრუნველყოფა.**
  - თუ ფასი ხელშემშლელია, გადაერთეთ უფრო იაფ ალტერნატივაზე.
- **მოითხოვეთ პაროლის დაცვა ორგანიზაციის ყველა მოწყობილობაზე, მათ შორის, პირად მობილურ მოწყობილობებზე, რომლებიც გამოიყენება სამსახურთან დაკავშირებული კომუნიკაციისათვის.**
- **ჩართეთ დისკის სრულად დაშიფვრა ყველა მოწყობილობაზე.**
- **ხშირად შეახსენეთ პერსონალს შეინახოს საკუთარი მოწყობილობები ფიზიკურად დაცულ ადგილას - და აღჭურვეთ თქვენი ოფისი შესაფერისი საკეტებით და კომპიუტერის უსაფრთხოების საშუალებებით.**
- **ნუ გააზიარებთ ფაილებს USB-ების გამოყენებით ან ჩართავთ USB-ებს თქვენს კომპიუტერებში.**
  - სანაცვლოდ გამოიყენეთ ფაილის გაზიარების ალტერნატიული უსაფრთხო ფუნქცია.

ფიშინგი: საყოველთაო საფრთხე მოწყობილობების და პროფილებისათვის

ფიშინგი მსოფლიოში წარმოადგენს ორგანიზაციებზე თავდასხმის ყველაზე უფრო გავრცელებულ და ეფექტურ მეთოდს. მეთოდი გამოიყენება, როგორც ყველაზე უფრო გამოცდილი სახელმწიფო სამხედრო სამსახურების, ისე თაღლითების მიერ.

ფიშინგს, მარტივად რომ ვთქვათ, ადგილი აქვს, როცა მეტოქე ცდილობს მოტყუებით გაგაზიარებინოთ ინფორმაცია, რომელიც შესაძლოა გამოყენებული იქნას თქვენს ან თქვენი ორგანიზაციის წინააღმდეგ. ფიშინგი შესაძლოა ელ-ფოსტით, ტექსტური შეტყობინებებით/SMS-ი (რომელსაც ხშირად SMS-ფიშინგს ან „სმიშინგს“ უწოდებენ), WhatsApp-ის მსგავსი შეტყობინების აპებით, სოციალურ მედიაში შეტყობინებებით ან პოსტებით ან სატელეფონო ზარებით (რომელსაც ხშირად ხმოვან ფიშინგს ან „ვიშინგს“ უწოდებენ). ფიშინგური შეტყობინებებით, შესაძლოა, ეცადონ ჩაგაწერინონ სენსიტიური ინფორმაცია (მაგ. პაროლები) ყალბ ვებგვერდზე, რათა მიიღონ წვდომა პროფილზე, გთხოვონ გააზიაროთ პირადი ინფორმაცია (მაგ. საკრედიტო ბარათის ნომერი) ზეპირად ან ტექსტურად ან დაგარწმუნონ ჩამოტვირთოთ საზიანო პროგრამა (საზიანო პროგრამული უზრუნველყოფა), რომელმაც შესაძლოა მოახდინოს თქვენი მოწყობილობის ინფიცირება. არატექნიკური მაგალითის სახით, ყოველდღიურად მილიონობით ადამიანი იღებს ყალბ ავტომატურ სატელეფონო ზარს, სადაც ეუბნებიან, რომ გატეხილია მათი საბანკო ანგარიში ან რომ მოპარულია მათი პირადობა - ყველა მათგანის მიზანია აიძულონ გაუთვითცნობიერებელი პირი გააზიაროს სენსიტიური ინფორმაცია.



როგორ შეგვიძლია ფიშინგის იდენტიფიკაცია?

ფიშინგი შესაძლოა ავბედითად და აღმოსაჩენად შეუძლებლად ჟღერს, თუმცა, არსებობს რამდენიმე მარტივი ნაბიჯი, რომელიც შესაძლოა გადადგას ყველამ თქვენს ორგანიზაციაში შეტევების უმეტესობისაგან დასაცავად. ფიშინგისაგან დაცვის ქვემოთ მოცემული რჩევები მოდიფიცირებული და აღებულია Freedom of the Press Foundation-ის მიერ შემუშავებული ფიშინგის სიღრმისეული სახელმძღვანელოდან, და გაცნობილი უნდა გაეცნოს თქვენს ორგანიზაციას (და სხვა კონტაქტებს) და უნდა ინტეგრირდეს თქვენს უსაფრთხოების გეგმაში.

ხანდახან, ველი „ვისგან“ გატყუებთ

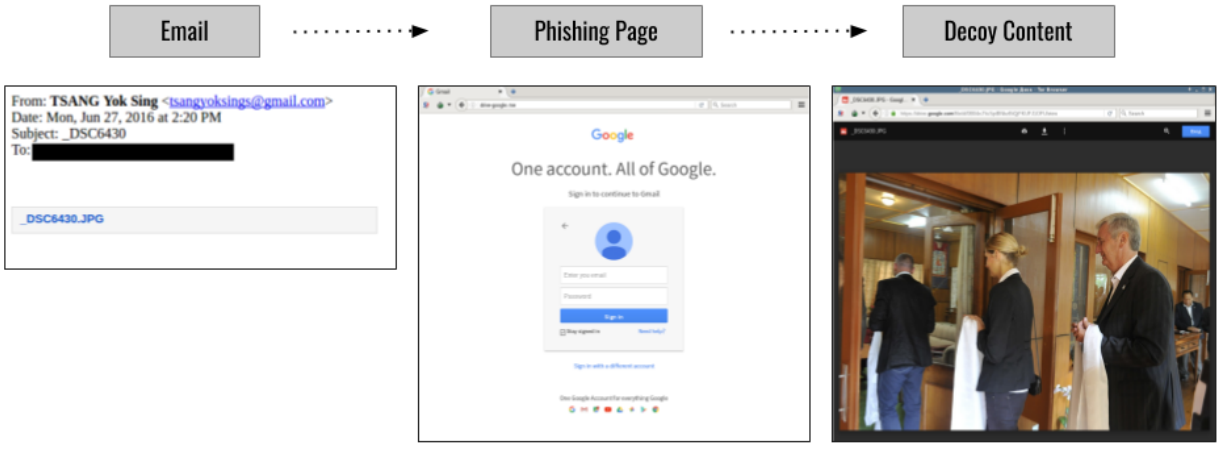
გაითვალისწინეთ, რომ თქვენი ელ-შეტყობინებების ველი „ვისგან“ შესაძლოა იყოს გაყალბებული, რათა შეგიყვანოთ შეცდომაში. ფიშერებისათვის ჩვეული ამბავია შეადგინონ ელ-ფოსტის მისამართი, რომელიც თქვენთვის ნაცნობია და ლეგიტიმურად გამოიყურება, თუმცა, მცირედ დამახინჯებულია. მაგალითად შესაძლოა, მიიღოთ ელწერილი ვიღაცისაგან მისამართით „john@gooogle.com“-ისა ნაცვლად „john@google.com”. ყურადღება მიაქციეთ ზედმეტ „O“-ს „google“-ში. ასევე შესაძლოა იცნობდეთ ვინმეს ელ-ფოსტის მისამართით „john@gmail.com”, თუმცა, მიიღოთ ფიშინგ ელ-შეტყობინება იმიტატორისაგან მისამართიდან „johm@gmail.com” - ერთადერთი განსხვავებაა ასოების შეუმჩნეველი ცვლილება ბოლოში. მუდამ გადაამოწმეთ, რომ იცნობთ ელ-შეტყობინების გამომგზავნ მისამართს ელ-შეტყობინების გახსნამდე. მსგავსი კონცეფცია ეხება ფიშინგს ტექსტის, ზარების თუ მესინჯერი აპების საშუალებით. თუ მიიღებთ შეტყობინებას უცნობი ნომრიდან, დაფიქრდით ორჯერ პასუხის გაცემამდე ან შეტყობინებაზე ინტერაქციამდე.



ფიშინგი და სამოქალაქო საზოგადოება

მახვილგონივრულ, პერსონალიზებულ ფიშინგურ შეტევებს ყოველდღიურად ადგილი აქვს სამოქალაქო საზოგადოების ჯგუფებზე მთელს მსოფლიოში.

ასეთი შეტევის ერთი მაგალითი მოცემულია The Citizen Lab-ის 2018 წ. ანგარიშში თვალყურის დევნება ბიუჯეტზე:ტიბეტური საზოგადოების წევრ სამიზნეებში ფიშინგის შეტევა. ეს მეტად იაფი და მარტივია - თუმცა, წარმოუდგენლად ეფექტური - ფიშინგური შეტევა მიმართული იყო ტიბეტში ადამიანის უფლებადამცველების და სხვა აქტივისტების წინააღმდეგ. შეტევა დაიწყო ფიშინგური ელ-შეტყობინებით (იხ. მარცხნივ) Gmail-ის სტანდარტული მისამართიდან, რომელიც შეიცავდა მხოლოდ ბმულს გამოსახულებით ფაილზე. დაწკაპუნების შემდეგ ბმულს სამიზნე გადაჰყავდა Google-ის ელ-ფოსტის სისტემაში ყალბ შესასვლელთან (იხ. შუაში), რომელიც გამოიყენებოდა პროფილის წვდომის პარამეტრების მოსაპარად. თუ მსხვერპლი შეიტანდა პარამეტრებს ყალბ გვერდზე, მისი პროფილი მარტივად იქნებოდა გატეხილი. საკუთარი მომხმარებლის სახელის და პაროლის ყალბ გვერდზე ჩაწერის შემდეგ მსხვერპლი გადამისამართდებოდა გამოსახულებაზე (იხ. მარჯვნივ), რომელზეც ნაჩვენები იყო ტიბეტში შეხვედრის დელეგატები. გამოსახულება გამოყენებული იყო სატყუარად, რათა ფიშინგის სამიზნეს დაეჯერებინა, რომ შევიდნენ Google-ში საკუთარ რეალურ პროფილზე და შემცირებულიყო შესაძლო ეჭვები ელ-შეტყობინების ნამდვილი საზიანო ხასიათის შესახებ.



უფრთხილდით დანართებს

დანართებში შესაძლოა იყოს საზიანო პროგრამა ან ვირუსი, რომლებიც, ჩვეულებრივ, თან სდევს ფიშინგ ელ-შეტყობინებებს. **დანართებიდან საზიანო პროგრამის თავიდან აცილების საუკეთესო მეთოდია მათი არასდროს ჩამოტვირთვა.** როგორც წესი, ნუ გახსნით რომელიმე დანართს დაუყონებლივ, განსაკუთრებით, თუ ისინი მიიღეთ თქვენთვის უცნობი ადამიანებისაგან. თუ შესაძლებელია, სთხოვეთ პიროვნებას, რომელმაც გამოგიგზავნათ დოკუმენტი გადაიტანოს ტექსტის ასლი ელწერილში ან გააზიაროს დოკუმენტი Google Drive-ის ან Microsoft OneDrive-ის მსგავსი სერვისის საშუალებით, რომლებსაც გააჩნია საკუთარ პლატფორმებზე ატვირთული თითქმის ყველა დოკუმენტის ვირუსზე სკანირება. დანერგეთ დანართების მიმართ უნდობლობის ორგანიზაციული კულტურა.
თუ დანართი აუცილებლად უნდა გახსნათ, ის უნდა გაიხსნას მხოლოდ უსაფრთხო გარემოში (იხ. სექცია „დამატებით“ ქვემოთ), სადაც შესაძლოა საზიანო პროგრამა ვერ გადავიდეს თქვენს მოწყობილობაზე.

თუ იყენებთ Gmail-ს და მიიღებთ დანართს ელ-შეტყობინებით, მისი თქვენს კომპიუტერში ჩამოტვირთვის და გახსნის ნაცვლად უბრალოდ დააწკაპუნეთ დართულ ფაილზე და წაიკითხეთ „preview”-ი თქვენს ბრაუზერში. აღნიშნული ნაბიჯი საშუალებას მოგცემთ გაეცნოთ ფაილის ტექსტს და შინაარსს მისი ჩამოტვირთის და მისთვის თქვენს კომპიუტერში შესაძლო საზიანო პროგრამის ჩატვირთვის გარეშე. ეს კარგი მეთოდია word-ის, PDF-ის და სლაიდებით პრეზენტაციების ფაილებისთვისაც კი. თუ გესაჭიროებათ დოკუმენტის რედაქტირება, გახსენით ფაილი ქლაუდ-პროგრამით, როგორიცაა Google Drive-ი და მოახდინეთ ფაილის კონვერტაცია Google Doc-ად ან Google Slides-ად.

თუ იყენებთ Outlook-ს, შეგიძლიათ მსგავსად წინასწარ იხილოთ დანართები მათი Outlook-დან ჩამოტვირთვის გარეშე. თუ გესაჭიროებათ დანართის რედაქტირება, გახსენით ის OneDrive-ში, თუ ის ხელმისაწვდომია თქვენთვის. თუ იყენებთ Yahoo Mail-ს, ქმედითია იგივე კონცეფცია. ნუ ჩამოტვირთავთ დანართებს, არამედ წინასწარ იხილეთ ისინი ვებ ბრაუზერის საშუალებით.

მიუხედავად იმისა თუ რა ინსტრუმენტებია თქვენთვის ხელმისაწვდომი, საუკეთესო მიდგომაა უბრალოდ არასდროს ჩამოტვირთოთ დანართები, რომლებიც უცნობია ან რომლებსაც არ ენდობით და მიუხედავად იმისა რამდენად მნიშვნელოვნად შესაძლოა გამოიყურებოდეს დანართი, არასდროს გახსნათ რაიმე თქვენთვის უცნობი ან მანამდე გამოუყენებელი ფაილის ტიპით.



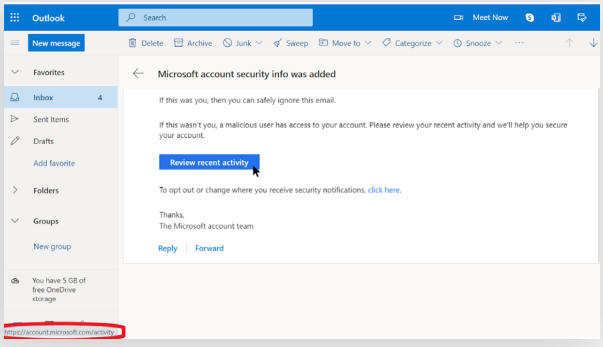
ფიშინგისაგან დაცვა თქვენი ორგანიზაციისათვის

თუ თქვენი ორგანიზაცია იყენებს კორპორაციულ Microsoft 365-ს ელ-შეტყობინებებისათვის და სხვა აპლიკაციებს, თქვენმა დომენის ადმინისტრატორმა უნდა შეიმუშაოს **უსაფრთხო დანართების პოლიტიკა** სახიფათო დანართებისაგან თავის დასაცავად. თუ იყენებთ კორპორაციულ Google Workspace-ს (მანამდე ცნობილი, როგორც GSuite-ი), არსებობს მსგავსად ეფექტური ოფცია, რომელიც უნდა შეიმუშაოს თქვენმა ადმინისტრატორმა და მას **Google Security Sandbox-ი** ეწოდება. უფრო გამოცდილ ინდივიდუალურ მომხმარებლებს შეუძლიათ იფიქრონ რთული სენდბოქს პროგრამების გამართვაზე, როგორიცაა **Dangerzone-ი** ან, მათთვის, ვისაც აქვთ Windows 10-ის პრო- ან კორპორაციული ვერსია, **Windows Sandbox-ი**.
კიდევ ერთი გასათვალისწინებელი მოწინავე ოფციაა თქვენს ორგნიზაციაში დომენის დასახელების დაცული სისტემის (DNS-ი) გაფილტვრის სერვისი. ორგანიზაციებს შეუძლიათ გამოიყენონ ხსენებული ტექნოლოგია, რათა დაბლოკონ მასალა შემთხვევით დაშვებული ან ინტერაქციაში მოხვედრილი საზიანო კონტენტიდან, რაც იძლევა ფიშინგისაგან დაცვის დამატებით შრეს. ახალი სერვისები, როგორიცაა **Cloudflare’s Gateway-ი**, აძლევს ასეთ შესაძლებლობებს ორგანიზაციებს დიდი თანხების მოთხოვნის გარეშე (Gateway-ი, მაგალითად, უფასოა 50-მდე მომხმარებლის შემთხვევაში). დამატებითი უფასო ინსტრუმენტები, მათ შორის, Global Cyber Alliance-ის კომპლექტის **Quad9-ი** გეხმარებათ დაბლოკოთ წვდომა ცნობილ დავირუსებულ ან სხვა საზიანო პროგრამების მომცველ გვერდებზე და შესაძლოა დააყენოთ ხუთ წუთზე ნაკლებ დროში.

ფრთხილად დაწკაპუნებისას

სკეპტიკურად შეაფასეთ ბმულები ელწერილებში ან სხვა ტექსტურ შეტყობინებებში. ბმულები შესაძლოა შენიღბული იყოს საზიანო ფაილების ჩამოსატვირთად ან გადაგიყვანოთ ყალბ გვერდებზე, სადაც შესაძლოა გთხოვონ პაროლის ან სხვა სენსიტიური ინფორმაციის მიწოდება. კომპიუტერთან მიმართებაში არსებობს მარტივი ეშმაკობა იმაში დასარწმუნებლად, რომ ელ-შეტყობინებაში ან შეტყობინებაში მოცემული ბმული გადაგაგზავნით ნავარაუდევ ადგილას: გამოიყენეთ მაუსი და მიიტანეთ ბმულზე დაწკაპუნებამდე და ნახეთ თქვენი ბრაუზერის ფანჯრის ძირში რეალური URL (იხ. სურათი ქვემოთ).

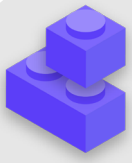
უფრო რთულია ბმულების შემოწმება მობილური აპარატით მიღებულ ელ-შეტყობინებაში მათზე შემთხვევით დაწკაპუნების გარეშე - ამიტომ იყავით ყურადღებით. შეგიძლიათ შეამოწმოთ ბმულის დანიშნულების პუნქტი სმარტფონების უმეტესობაში ბმულზე ხანგრძლივი დაჭერით (შეკავებით) მანამ, სანამ არ გამოჩნდება სრული URL-ი.
SMS-ით და მესინჯერით ფიშინგისას შემოკლებული ბმულები მეტად გავრცელებული პრაქტიკაა URL-ის დანიშნულების პუნქტის შესანიღბად. თუ ხედავთ მოკლე ბმულს (მაგ., bit.ly-ი ან tinyurl.com-ი) ნავვლად სრული URL-ის, არ დააწკაპუნოთ მასზე. თუ ბმული მნიშვნელოვანია, გადაიტანეთ მისი ასლი URL-ის გამაფართოებელში, როგორიცაა **https://www.expandurl.net/**, რათა ნახოთ შემოკლებული URL-ის რეალური დანიშნულების პუნქტი. გარდა ამისა, ნუ დააწკაპუნებთ თქვენთვის უცნობი ვებგვერდების ბმულებზე. ეჭვის შემთხვევაში მოიძიეთ გვერდი ბრჭყალებში გვერდის დასახელებით (მაგ.: “www.badwebsite.com”-ი), რათა ნახოთ არის თუ არა ის ლეგიტიმური გვერდი. ასევე შეგიძლიათ გაატაროთ პოტენციურად საეჭვო ბმულები **VirusTotal**-ის URL-ის სკანერში. ეს არაა 100 პროცენტიანი გარანტია, თუმცა, სიფრთხილის მისაღებად ღირებული ნაბიჯია.



და ბოლოს, თუ დააწკაპუნებთ შეტყობინებაში მოცემულ ნებისმიერ ბმულზე და გთხოვენ შეხვიდეთ რომელიმე სისტემაში, არ გააკეთოთ ეს, სანამ არ იქნებით 100 პროცენტით დარწმუნებული, რომ ელ-შეტყობინება ლეგიტიმურია და გადაგაგზავნით შესაფერის გვერდზე. არაერთი ფიშინგური შეტევა გაწვდით ბმულებს, რომლებიც გადაგაგზავნით Gmail-ის, Facebook-ის თუ სხვა პოპულარული ვებგვერდების სისტემაში შესვლის ყალბ გვერდებზე. ნუ წამოეგებით ანკესზე. მუდამ შეგიძლიათ გახსნათ სხვა ბრაუზერი და თავად პირდაპირ გადახვიდეთ ნაცნობ გვერდზე, როგორიცაა Gmail.com, Facebook.com და სხვა, თუ გსურთ ან გესაჭიროებათ სისტემაში შესვლა. ეს ასევე მიგიყვანთ კონტენტამდე, უსაფრთხოდ – რა თქმა უნდა, თუ ის იყო ლეგიტიმური.

როგორ მოვიქცეთ ფიშინგური შეტყობინების მიღებისას?

თუ ვინმე თქვენს ორგანიზაციაში მიიღებს არასასურველ დანართს, ბმულს, გამოსახულებას ან სხვა მხრივ საეჭვო შეტყობინებას ან ზარს, მნიშვნელოვანია, რომ მან დაუყონებლივ აცნობოს მის შესახებ თქვენს ორგანიზაციაში IT-ის უსაფრთხოებაზე პასუხისმგებელ პირს. თუ არ გყავთ ასეთი პირი, უნდა გამოყოთ ასეთი პირი უსაფრთხოების თქვენი გეგმის შემუშავების პროცესში. პერსონალს ასევე შეუძლია აცნობოს ელ-შეტყობინების, როგორც სპამის ან ფიშინგის შესახებ უშუალოდ Gmail-ში ან Outlook-ში. უმნიშვნელოვანესია იქონიოთ გეგმა, თუ როგორ უნდა მოიქცეს პერსონალი ან მოხალისეები, როდესაც მიიღებენ შესაძლო ფიშინგ შეტყობინებას. გარდა ამისა, გირჩევთ დანერგოთ ფიშინგთან ბრძოლის ხსენებული აღიარებული მეთოდიკა - არ დააწკაპუნოთ საეჭვო ბმულებზე, თავი აარიდოთ დანართებს და შეამოწმოთ მისამართი ველში „ვისგან“ - და გაუზიაროთ ისინი მათ, ვინც მუშაობს თქვენთან, სასურველია ფართოდ გამოყენებული საკომუნიკაციო არხებით. ხსენებული უჩვენებს, რომ ზრუნავთ ხალხზე, რომელთანაც ხართ კომუნიკაციაში და ახალისებს კულტურას თქვენს საზოგადოებაში ფიშინგის საფრთხის გაცნობიერებით. თქვენი უსაფრთხოება დამოკიდებულია ორგანიზაციებზე, რომლებსაც ენდობით და პირიქით. უკეთესი მეთოდიკა იცავს ყველას.
გარდა ზემოთ მოცემული რჩევების პერსონალისა და მოხალისეებისათვის გაზიარებისა, ასევე შეგიძლიათ დანერგოთ ფიშინგის იდენტიფიკაცია **Google Phishing Quiz-ით**. ასევე დაბეჯითებით გირჩევთ გამართოთ პერსონალის რეგულარული ტრენინგი ფიშინგის საკითხებზე, რათა შემოწმდეს ინფორმირებულობა, ხოლო ხალხი იყოს ფხიზლად. აღნიშნულ ტრენინგს შესაძლოა მიეცეს ოფიციალური სახე, როგორც რეგულარულად ორგანიზებული შეხვედრების ნაწილი ან გაიმართოს უფრო არაოფიციალურ ატმოსფეროში. მნიშვნელოვანია, რომ მთელი ორგანიზაცია კომფორტულად გრძნობდეს თავს ფიშინგის შესახებ კითხვების დასმისას, მის თაობაზე ინფორმირებისას (მაშინაც კი, როცა გრძნობენ, რომ შესაძლოა დაუშვეს შეცდომა, როგორიცაა ბმულზე დაწკაპუნება) და რომ შეეძლოს დაგეხმაროთ თქვენი ორგანიზაციის დაცვაში ხსენებული ძლიერი გავლენის და საფრთხის მაღალი ალბათობისაგან.



ფიშინგი

- **აწარმოეთ პერსონალის რეგულარული ტრენინგი მასზედ, თუ რა არის ფიშინგი, როგორ ამოვიცნოთ ის და დავიცვათ მისგან თავი, მათ შორის, ფიშინგი ტექსტურ შეტყობინებებში, მესინჯერებში და სატელეფონო ზარებში და არა მხოლოდ ელ-შეტყობინებებში.**
- **ხშირად შეახსენეთ პერსონალს იმ აღიარებული მეთოდების შესახებ, როგორიცაა:**
  - ნუ ჩამოტვირთავთ უცნობ ან პოტენციურად საეჭვო დანართებს.
  - შეამოწმეთ ბმულის URL-ი დაწკაპუნებამდე. ნუ დააწკაპუნებთ უცნობ ან პოტენციურად საეჭვო ბმულებზე.
  - ნუ მიაწვდით სენსიტიურ ან პირად ინფორმაციას ელ-ფოსტით, ტექსტით ან ტელეფონის ზარით უცნობ ან დაუდასტურებელ მისამართებს ან ხალხს.
- **წაახალისეთ ფიშინგის შესახებ რეპორტინგი.**
  - დაადგინეთ დარეპორტების მექანიზმი და ორგანიზაციაში ფიშინგზე პასუხისმგებელი პირი.
  - წაახალისეთ რეპორტინგი და ნუ დასჯით წარუმატებლობისას.



უსაფრთხო კომუნიკაცია და მონაცემების შენახვა

კომუნიკაცია და მონაცემების გაზიარება

თქვენი ორგანიზაციისათვის კომუნიკაციის შესახებ საუკეთესო გადაწყვეტილებების მისაღებად, უმნიშვნელოვანესია გესმოდეთ დაცვის სხვადასხვა ტიპი, რომელიც ხელმისაწვდომია ჩვენი კომუნიკაციისათვის, და რატომაა ხსენებული დაცვა მნიშვნელოვანი.

კომუნიკაციის უსაფრთხოების ერთ-ერთი უმნიშვნელოვანესი ელემენტი დაკავშირებულია პირადი კომუნიკაციის კონფიდენციალურობის დაცვა - რომელსაც ჩვენს დროში დიდი ყურადღება ეთმობა დაშიფვრის გზით. სათანადო დაშიფვრის გარეშე შიდა კომუნიკაცია ხილვადი შესაძლოა ყოფილიყო მეტოქეების ნებისმიერი რიცხვისათვის. დაუცველმა კომუნიკაციამ შესაძლოა გაამჟღავნოს სენსიტიური ან უხერხული ინფორმაცია და შეტყობინებები, გაამჟღავნოს პაროლები ან სხვა პირადი მონაცემები და შეუქმნას რისკი თქვენს პერსონალს და ორგანიზაციას გამომდინარე თქვენი კომუნიკაციის ხასიათიდან და თქვენს მიერ გაზიარებული კონტენტიდან.

უსაფრთხო კომუნიკაცია და სამოქალაქო საზოგადოება

დემოკრატიის და ადამიანის უფლებებისათვის მებრძოლი ათასობით აქტივისტი და ორგანიზაცია ეყრდნობა უსაფრთხო კომუნიკაციის არხებს ყოველდღიურად, რათა დაიცვას კონფიდენციალობა კონკურენტულ პოლიტიკურ გარემოში. უსაფრთხოების მეთოდიკის გარეშე სენსიტიური შეტყობინებები შესაძლოა ხელყოფილი და გამოყენებული იქნეს წუყებების მიერ აქტივისტებზე ზემოქმედების და პროტესტის ჩახშობის მიზნით. აღნიშნულის ერთი ცნობილ და სათანადოდ დოკუმენტირებულ მაგალითს ადგილი ჰქონდა ბელორუსში 2010 არჩევნების შედეგად. როგორც დეტალურად აღწერილია Amnesty International-ის ანგარიშში, სატეფონო ზარები და სხვა დაუშიფრავი კომუნიკაცია ხელყოფილი და სასამართლოში გამოყენებული იქნა ხელისუფლების მიერ გამოჩენილი ოპოზიციონერი პოლიტიკოსების და აქტივისტების წინააღმდეგ, რომელთაგან მრავალმა წლები გაატარა ციხეში. 2020 წელს ბელარუსში არჩევნების შემდგომი საპროტესტო აქციების ათასობით მონაწილემ გამოიყენა მომხმარებელზე ორიენტირებული უსაფრთხო მესინჯერები, რომლებიც არ იყო ადვილად ხელმისაწვდომი ჯერ კიდევ ათი წლით ადრე მათი სენსიტიური კომუნიკაციის დასაცავად.



რა არის დაშიფვრა და რატომაა ის მნიშვნელოვანი?

დაშიფვრა მათემატიკური პროცესია, რომელიც გამოიყენება შეტყობინების ან ფაილის „სკრემბლინგში“ ისე, რომ მხოლოდ გასაღების მქონე პირს ან ორგანიზაციას შეეძლოა მისი „გაშიფვრა“ და წაკითხვა. Electronic Frontier Foundation-ის „თვალთვალისაგან თავდაცვის სახელმძღვანელო“ პრაქტიკულად (მათ შორის, გრაფიკულად) ხსნის, რას გულისხმობს დაშიფვრა:

დაუშიფრავი შეტყობინებები

რაიმე დაშიფვრის გარეშე, სეტყობინების გადაცემის ყველა მონაწილეს და ყველას, ვისაც შეუძლია უთვალთვალოს მას მოძრაობისას, შეუძლია გაეცნოს მის შინაარსს. ამას შესაძლოა არ ჰქონდეს მნიშვნელობა, თუ მხოლოდ „სალამს“ აბობთ, თუმცა, ეს შესაძლოა დიდი საქმე იყოს, თუ აგზავნით რაიმ უფრო პრივატულს ან სენსიტიურს, რაც არ გსურთ, ნახოს თქვენმა ტელეკომ-პროვაიდერმა, ISP-მა, არაკეთილმოსურნე ხელისუფლებამ ან ნებისმიერმა სხვა მეტოქეთ. ამის გამო, მნიშვნელოვანია თავიდან აიცილოთ რაიმე სენსიტიური შეტყობინების (და, საუკეთესო შემთხვევაში, საერთოდ ნებისმიერი შეტყობინების) დაუშიფრავი ინსტრუმენტებით გაგზავნა. გახსოვდეთ, რომ კომუნიკაციის ზოგიერთი პოპულარული მეთოდი - როგორიცაა SMS-ი და სატელეფონო ზარები - მუშაობს პრაქტიკულად რაიმე დაშიფვრის გარეშე (როგორც სურათზე ამ ნაჩვენები).



როგორც ზედა სურათზე ჩანს, სმარტფონი უგზავნის მწვანე, დაუშიფრავ ტექსტურ შეტყობინებას („სალამი“) მეორე, ბოლო მარჯვენა სმარტფონს. გზაში ფიჭური კავშირის ანძა (ან, რაიმეს ინტერნეტით გაგზავნისას, თქვენი ინტერნეტ-პროვაიდერი, რომელსაც ISP ეწოდება) გადასცემს შეტყობინებას კომპანიის სერვერებით. აქედან ის ქსელის საშუალებით გადადის სხვა ფიჭური კავშირის ანძაზე, რომელსაც შეუძლია დაინახოს დაუშიფრავი შეტყობინება „სალამი“, ბოლოს კი მიმართოს საბოლოო დანიშნულებისაკენ. უნდა აღინიშნოს, რომ რაიმე დაშიფვრის გარეშე, ყველას, ვინც მონაწილეობს შეტყობინების გადაცემაში და ყველას, ვისაც შეუძლია უთვალთვალოს მას გავლისას, შეუძლია მისი შინაარსის ნახვა. ამას შესაძლოა არ ჰქონდეს მნიშვნელობა, თუ მხოლოდ „სალამს“ ამბობთ, თუმცა, ეს შესაძლოა დიდი პრობლემა იყოს, თუ აგზავნით რაიმე უფრო კონფიდენციალურს ან სენსიტიურს, რაც არ გსურთ ნახოს თქვენმა ტელეკომ-პროვაიდერმა, ISP-მა, არაკეთილმოსურნე ხელისუფლებამ ან ნებისმიერმა სხვა მეტოქემ. ამის გამო, მნიშვნელოვანია თავიდან აიცილოთ რაიმე სენსიტიური შეტყობინების (და, საუკეთესო შემთხვევაში, საერთოდ ნებისმიერი შეტყობინების) დაუშიფრავი ინსტრუმენტებით გაგზავნა. გახსოვდეთ, რომ კომუნიკაციის ზოგიერთი პოპულარული მეთოდი - როგორიცაა SMS-ი და სატელეფონო ზარები - მუშაობს პრაქტიკულად რაიმე დაშიფვრის გარეშე (როგორც ზემოთ სურათზეა ნაჩვენები).

არსებობს მოძრაობისას მონაცემთა დაშიფვრის ორი გზა: ***სატრანსპორტო შრის დაშიფვრა*** და ***აბონენტური დაშიფვრა***. მნიშვნელოვანია იცოდეთ პროვაიდერის მიერ მხარდაჭერილი დაშიფვრის სერვისის ტიპი, რამდენადაც თქვენი ორგანიზაცია აკეთებს არჩევანს მიიღოს უფრო უსაფრთხო კომუნიკაციის მეთოდები და სისტემები. ხსენებული სხვაობა კარგადაა აღწერილია **„თვალთვალისაგან თავდაცვის სახელმძღვანელოს“** მიერ რომელიც კვლავ ადაპტირებულია ქვემოთ:

სატრანსპორტო შრის დაშიფვრა

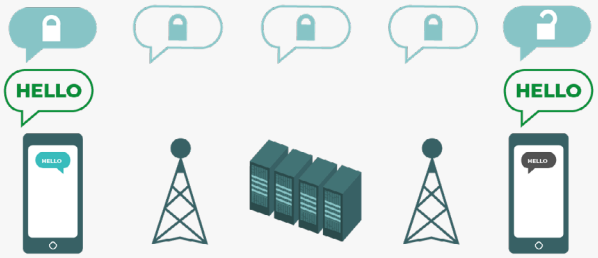
სატრანსპორტო შრის დაშიფვრა, ასევე ცნობილი, როგორც სატრანსპორტო შრის უსაფრთხოება (TLS-ი), იცავს შეტყობინებებს მათი თქვენი მოწყობილობიდან მესინჯერის სერვერებამდე და მათგან მიმღების მოწყობილობამდე მოძრაობის დროს. ეს იცავს მათ თქვენს ქსელში ან თქვენს ინტერნეტ- თუ ტელეკომუნიკაციის სერვისის პროვაიდერებთან მყოფი ჰაკერების ცნობისმოყვარე თვალისაგან. თუმცა, შუალედში, თქვენი მესინჯერის/ელ-ფოსტის სერვისის პროვაიდერი, ვებგვერდი, რომელსაც ნახულობთ ან აპი, რომელსაც იყენებთ ხედავს თქვენი შეტყობინებების დაშიფრულ ასლებს. რამდენადაც თქვენი შეტყობინებები შესაძლოა ხილვადი იყოს (და უფრო ხშირად ინახება) თქვენს სერვერებზე, ისინი შესაძლოა მოწყვლადი იყოს სამართალდამცველთა მოთხოვნებისათვის ან ქურდობისათვის, თუ კომპანიის სერვერები გატეხილია.



ზედა სურათი გვიჩვენებს სატრანსპორტო შრის დაშიფვრის მაგალითს. მარცხნივ სმარტფონი აგზავნის მწვანე, დაუშიფრავ შეტყობინებას: „სალამი“. ხსენებული შეტყობინება იშიფრება და შემდეგ გადაეცემა ფიჭური კავშირის ანძას. შუაში კომპანიის სერვერებს შეუძლიათ გაშიფრონ შეტყობინება, წაიკითხონ შინაარსი, გადაწყვიტონ სად გაგზავნონ ის, ხელახლა დაშიფრონ ის და გაგზავნონ სხვა ფიჭური კავშირის ანძაზე დანიშნულების პუნქტისაკენ. ბოლოს სხვა სმარტფონი იღებს დაშიფრულ შეტყობინებას და გაშიფრავს მას „სალამის“ წასაკითხად.

აბონენტური დაშიფვრა

აბონენტური დაშიფვრა იცავს შეტყობინებებს მთელ გზაზე გამგზავნიდან მიმღებამდე. ის უზრუნველყოფს რომ ინფორმაცია იქცეს საიდუმლო შეტყობინებად გამგზავნის მხრიდან (პირველი „ბოლო“) და გაიშიფრება მისი საბოლოო მიმღების მიერ (მეორე „ბოლო“). არავის, მათ შორის, აპს ან სერვისს, რომელსაც იყენებთ, შეუძლია „მიაყურადოს“ ან მოუსმინოს თქვენს ქმედებას.



ზედა სურათი გვიჩვენებს აბონენტური დაშიფვრის მაგალითს. მარცხნივ სმარტფონი აგზავნის მწვანე, დაუშიფრავ შეტყობინებას: „სალამი“. ხსენებული შეტყობინება იშიფრება და შემდეგ გადაეცემა ფიჭური კავშირის ანძას, შემდეგ კი აპის/სერვისის სერვერებს, რომლებსაც არ შეუძლიათ მისი შინაარსის წაკითხვა, მაგრამ გადასცემენ საიდუმლო შეტყობინებას მისი დანიშნულების პუნქტში. ბოლოს სხვა სმარტფონი იღებს დაშიფრულ შეტყობინებას და გაშიფრავს მას „სალამის“ წასაკითხად. განსხვავებით სატრანსპორტო შრის დაშიფვრისაგან, თქვენს ISP-ს ან მესინჯერის ჰოსტს არ შეუძლია შეტყობინების გაშიფვრა. გაშიფვრის გასაღები აქვთ და კითხულობენ შეტყობინებას მხოლოდ ბოლო პუნქტები (დაშიფრული შეტყობინებების გამგზავნი და მიმღები მოწყობილობები).

რა ტიპის დაშიფვრა გვჭირდება?

გადაწყვეტილების მიღებისას სატრანსპორტო შრის დაშიფვრა სჭირდება თქვენს ორგანიზაციას თუ აბონენტური დაშიფვრა (ან რაღაც ამ ორის რაღაც კომბინაცია განსხვავებული სისტემების და საქმიანობისათვის), დიდი კითხვის ნიშანი უნდა დაუსვათ ნდობას. მაგალითად, ენდობით თქვენ მიერ გამოყენებულ აპს ან სერვისს? ენდობით მის ტექნიკურ ინფრასტრუქტურას? გაშფოთებთ შესაძლებლობა, რომ არაკეთილმოსურნე ხელისუფლებას შეუძლია აიძულოს კომპანია გადასცეს თქვენი შეტყობინებები – და ამ შემთხვევაში ენდობით კომპანიის პოლიტიკას, დაგიცვათ სამართალდამცველების მოთხოვნებისაგან?
თუ პასუხი ყველა ხსენებულ კითხვაზე არის „არა“, მაშინ გესაჭიროებათ აბონენტური დაშიფვრა. თუ მათზე პასუხია „დიახ“, მაშინ გესაჭიროებათ სერვისი, რომელიც მხარს უჭერს მხოლოდ სატრანსპორტო შრის დაშიფვრას - მაგრამ, როცა შესაძლებელია, ჩვეულებრივ უკეთესია მიიღოთ სერვისი, რომელიც მხარს უჭერს სააბონენტო დაშიფვრას.

ჯგუფებში შეტყობინებების გაგზავნისას გახსოვდეთ, რომ თქვენი შეტყობინებების უსაფრთხოება იმდენად მაღალია, რამდენადაც მაღალია შეტყობინების ყველა მიმღების უსაფრთხოება.
გარდა დაცული აპების და სისტემების ყურადღებით არჩევისა, მნიშვნელოვანია, რომ ჯგუფის ყველა წევრი იყენებდეს სხვა აღიარებულ მეთოდიკას პროფილის და მოწყობილობის უსაფრთხოების შესახებ. საკმარისია ერთი ცუდი თანამშრომელი ან ერთი ინფიცირებული მოწყობილობა, რომ ადგილის ჰქონდეთ ჯგუფური ჩატის ან ზარის მთელი კონტენტის გაჟონვას.

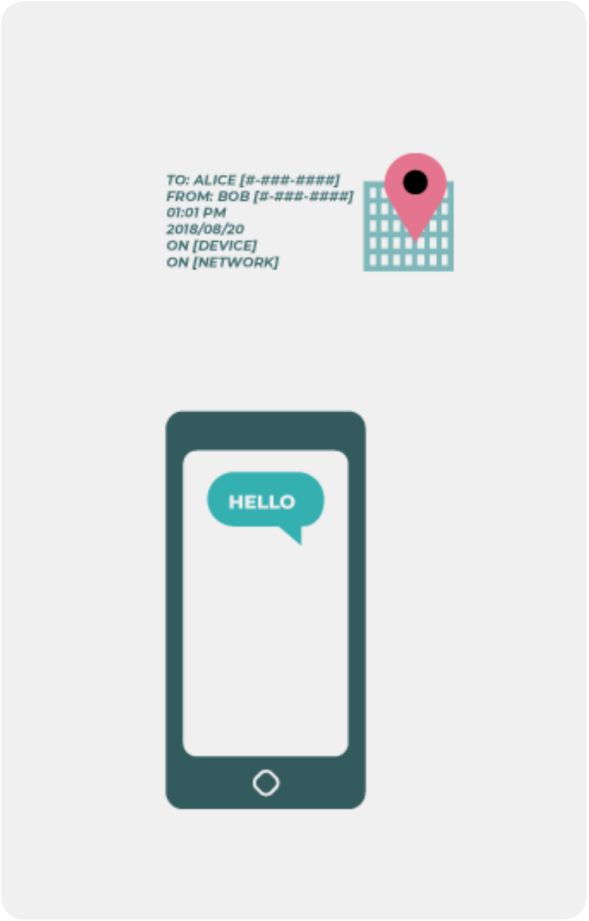
მესინჯერის აბონენტური დაშიფვრის რომელი ინსტრუმენტები უნდა გამოვიყენოთ (2022 წლიდან)?

თუ გესაჭიროებათ აბონენტური დაშიფვრა ან უბრალოდ გსურთ მიიღოთ აღიარებული მეთოდიკა მიუხედავად თქვენი ორგანიზაციის წინაშე არსებული საფრთხისა, აქ არის რამდენიმე სანდო სერვისის მაგალითი, რომლებიც, **2022 წლიდან,** გთავაზობთ მესინჯერს და ზარებს აბონენტური დაშიფვრით. სახელმძღვანელოს მოცემული სექცია განახლდება ონლაინ რეგულარულად, თუმცა, გაითვალისწინეთ, რომ დაცული შეტყობინებების სამყაროში ყველაფერი იცვლება სწრაფად, ამდენად, აღნიშნული რეკომენდაციები, შესაძლოა, აღარ იყოს თანამედროვე მოცემული სექციის თქვენს მიერ წაკითხვისას. გახსოვდეთ, რომ თქვენი კომუნიკაცია მხოლოდ იმდენადაა უსაფრთხო, რამდენადაც თავად თქვენი მოწყობილობა. ამგვარად, გარდა შეტყობინებების უსაფრთხო მეთოდიკის დამკვიდრებისა, მნიშვნელოვანია აღიარებული პრაქტიკა, აღწერილი წინამდებარე სახელმძღვანელოს სექციაში [დაცული მოწყობილობები](#).

კომუნიკაციის აბონენტური დაშიფვრის რეკომენდებული ინსტრუმენტები

ტექსტური მესინჯერი (ინდივიდუალური ან ჯგუფური)	• **Signal** • **WhatsApp (მხოლოდ ქვემოთ დეტალურად აღწერილი სპეციალური პარამეტრებით კონფიგურაციით)**
აუდიო და ვიდეო ზარები	• **Signal (40-მდე პიროვნება)** • **WhatsApp (32-მდე პიროვნება აუდიო, რვა - ვიდეო)**
ფაილების გაზიარება	• **Signal** • **Keybase / Keybase Teams** • **OnionShare + Signal-ის მსგავსი მესინჯერი აპი აბონენტური დაშიფვრით**

რა არის მეტამონაცემები და უნდა ვიყოთ თუ არა შეშფოთებული მის გამო?



ვის ესაუბრებით თქვენ და თქვენი პერსონალი და როდის და სად ესაუბრებით მათ ხშირად შესაძლოა ისევე სენსიტიური იყოს, როგორც რაზე ესაუბრებით. მნიშვნელოვანია გვახსოვდეს, რომ აბონენტური დაშიფვრა იცავს მხოლოდ თქვენი კომუნიკაციის შინაარსს („რა"). სწორედ აქ ერთვება *მეტამონაცემები*. EFF-ის „თვალთვალისაგან თავდაცვის სახელმძღვანელო" მიმოიხილავს მეტამონაცემებს და იმას, თუ რატომ აქვს მას მნიშვნელობა ორგანიზაციებისათვის (მათ შორის, იმის ილუსტრაცია, თუ როგორ გამოიყურება მეტამონაცემები):

მეტამონაცემები ხშირად აღწერილია, როგორც ყველაფერი, გარდა თქვენი კომუნიკაციის შინაარსისა. შეგიძლიათ, იფიქროთ მეტამონაცემებზე, როგორც კონვერტის ციფრულ ექვივალენტზე. ზუსტად როგორც კონვერტი მოიცავს ინფორმაციას გამგზავნის, მიმღების და შეტყობინების დანიშნულების ადგილის შესახებ, ისე მოიცავს მათ მეტამონაცემები. მეტამონაცემები წარმოადგენს ინფორმაციას თქვენ მიერ გაგზავნილი და მიღებული კომუნიკაციის შესახებ.

მეტამონაცემების ზოგიერთი მაგალითი მოიცავს:
- ვინ ვისთან აწარმოებს კომუნიკაციას
- თქვენი ელ-შეტყობინებების საგნის ველი
- თქვენი საუბრის ხანგრძლივობა
- დრო, როცა ადგილი ჰქონდა საუბარს
- თქვენი ლოკაცია კომუნიკაციისას

მეტამონაცემების პაწაწინა ნიმუშსაც კი შეუძლია წარმოაჩინოს თქვენი ორგანიზაციის საქმიანობის ახლო ხედი. მოდით ვნახოთ თუ რამდენად ინფორმატიული შესაძლოა იყოს მეტამონაცემები ჰაკერების, სამთავრობო უწყებების და კომპანიებისათვის, რომლებიც აგროვებენ მათ:

მათ იციან, რომ დაურეკეთ ჟურნალისტს და ესაუბრეთ მას ერთი საათის განმავლობაში, სანამ ეს ჟურნალისტი გამოაქვეყნებდა ამბავს ანონიმი ავტორის ციტირებით. თუმცა, მათ არ იციან რაზე საუბრობდით.

მათ ბევრი იციან იმის შესახებ, რომ თქვენი ორგანიზაცია დაუკავშირდა ციფრული უსაფრთხოების ცნობილ ადგილობრივ ტრენერს. თუმცა, შეტყობინებების თემა უცნობია.

მათ იციან, რომ მიიღეთ ელ-შეტყობინება COVID-ის ტესტირების სამსახურიდან, შემდეგ დაურეკეთ თქვენს ექიმს, შემდეგ ეწვიეთ ჯანმრთელობის მსოფლიო ორგანიზაციის ვებგვერდს იმავე საათის განმავლობაში. თუმცა, მათ არ იციან ელ-შეტყობინების თუ ტელეფონით საუბრის შინაარსი.

მათ იციან, რომ მიიღეთ ელ-შეტყობინება ადამიანის უფლებების დამცველი ადგილობრივი ჯგუფისაგან, რომლის საგანი იყო „გააგებინეთ მთავრობას: მოეშვას თქვენს დევნას". თუმცა, ელ-შეტყობინების შინაარსი მათთვის უხილავია.

მეტამონაცემები არაა დაცული დაშიფვრით მესინჯერების უმეტესობის მიერ. მაგალითად, თუ აგზავნით შეტყობინებას WhatsApp-ით, გახსოვდეთ, რომ თქვენი შეტყობინების შინაარსი დაშიფრულია აბონენტური დაშიფვრით, მაგრამ მაინც შესაძლოა ვინმემ იცოდეს ვის უგზავნით შეტყობინებებს, რამდენად ხშირად და რამდენ ხანს ესაუბრებით ვინმეს ტელეფონით. შედეგად, უნდა გახსოვდეთ, თუ რა რა რისკი არსებობს (ასეთის არსებობის შემთხვევაში), თუ კონკრეტულ მეტოქეებს შეუძლიათ გაარკვიონ ვის ესაუბრა ორგანიზაცია, როდის ესაუბრეთ მათ და (ელ-შეტყობინების შემთხვევაში) თქვენი ორგანიზაციის კომუნიკაციის ზოგადი საგანი თუ თემა.

ერთ-ერთი მიზეზი, რის გამოც ასე გულდასმით გირჩევთ **Signal-ს** არის ის, რომ გარდა აბონენტური დაშიფვრის უზრუნველყოფისა, მან **დანერგა ფუნქციები და იკისრა იმ მეტამონაცემების შემცირების ვალდებულება, რომლებსაც აღრიცხავს და ინახავს**. მაგალითად, Signal-ის ფუნქცია Sealed Sender დაშიფრავს მეტამონაცემებს, თუ ვინ ვის ესაუბრება ისე, რომ Signal-მა იცის შეტყობინების მიმღები და არ იცის გამგზავნი. ჩვეულებრივ, ხსენებული ფუნქცია მუშაობს მხოლოდ არსებულ კონტაქტებთან თუ პროფილებთან (ხალხთან) კომუნიკაციისას, ვისთანაც უკვე გქონიათ კომუნიკაცია ან ვინც უკვე არის თქვენი კონტაქტების სიაში. თუმცა, შეგიძლიათ, ჩართოთ პარამეტრი Sealed Sender და დააყენოთ „ყველასგან დაშვება“, თუ თქვენთვის მნიშვნელოვანია, რომ Signal-ში ყველა საუბრიდან, მათ შორის, თქვენთვის უცნობ ადამიანებთან საუბრებიდანაც კი გამორიცხოთ ასეთი მეტამონაცემები.

რას იტყვით ელ-ფოსტაზე?

ელ-ფოსტის პროვაიდერების უმეტესობა, მაგალითად Gmail-ი, Microsoft Outlook-ი და Yahoo Mail-ი, იყენებს სატრანსპორტო შრის დაშიფვრას. ამგვარად, თუ უნდა აწარმოოთ სენსიტიური კონტენტის კომუნიკაცია ელ-ფოსტის გამოყენებით და შეშფოთებული ხართ, რომ ელ-ფოსტის თქვენს პროვაიდერს შესაძლოა კანონით მოეთხოვოს მიაწოდოს ინფორმაცია ხელისუფლებას ან სხვა მეტოქეს თქვენი კომუნიკაციის შესახებ, შესაძლოა გერჩივნოთ აბონენტური დაშიფვრით ელ-ფოსტის გამოყენება. თუმცა, გახსოვდეთ, რომ აბონენტური დაშიფვრით ელ-ფოსტის გამოყენებაც კი მაინც არ არის სრულყოფილი უსაფრთხოების თვალსაზრისით, მაგალითად, ელ-შეტყობინებების დაუშიფრავი საგნის ველები და მეტამონაცემების დაუცველობა. თუ გესაჭიროებათ კონკრეტული სენსიტიური ინფორმაციის კომუნიკაცია, ელ-ფოსტა არაა საუკეთესო არჩევანი. ამის ნაცვლად მიმართეთ Signal-ის მსგავს უსაფრთხოდ შეტყობინებების გაგზავნის შესაძლებლობებს.

თუ თქვენი ორგანიზაცია კვლავაც იყენებს ელ-ფოსტას, უმნიშვნელოვანესია, შემოიღოთ ორგანიზაციული სისტემა. აღნიშნული გეხმარებათ საყოველთაო რისკების შეზღუდვაში, რომლებიც წარმოიშვება პერსონალის მიერ სამსახურეობრივი მიზნით ელ-ფოსტის პირადი მისამართების გამოყენებისას, რაც წარმოადგენს უსაფრთხოების სუსტ მეთოდიკას. მაგალითად, პერსონალისათვის ორგანიზაციის მიერ შექმნილი ელ-ფოსტის პროფილების გადაცემით შეგიძლიათ დანერგოთ აღიარებული მეთოდიკა, როგორიცაა თქვენი ორგანიზაციის მიერ მართული პროფილების ძლიერი პაროლები და 2FA. თუ, თანახმად ზემოთ მოცემული თქვენი ანალიზისა, აბონენტური დაშიფვრა აუცილებელია თქვენი ელ-ფოსტისათვის, როგორც Protonmail-ი, ისე Tutanota-ი გთავაზობთ სქემებს ორგანიზაციებისათვის. თუ სატრანსპორტო შრის დაშიფვრა ადექვატურია თქვენი ორგანიზაციის ელ-ფოსტისათვის, შესაძლოა გამოსადეგი იყოს სქემები, როგორიცაა Google Workspace-ი (Gmail-ი) ან Microsoft 365-ი (Outlook-ი).

შეგვიძლია ბოლომდე ვენდოთ WHATSAPP-ს?

WhatsApp-ი წარმოადგენს პოპულარულ არჩევანს უსაფრთხო მესინჯერისათვის და შესაძლოა კარგი ოფცია იყოს გამომდინარე მისი საყოველთაობიდან. ზოგიერთები შეშფოთებულნი არიან, რომ მას ფლობს და აკონტროლებს Facebook-ი, რომელიც მუშაობდა მის სხვა კუთვნილ სისტემებში ინტეგრაციაზე. ზოგიერთი ასევე შეშფოთებულია მეტამონაცემების იმ რაოდენობით (მაგ. ინფორმაცია იმის შესახებ, თუ ვისთან და როდის გქონდათ კომუნიკაცია), რომელსაც აგროვებს WhatsApp-ი. თუ გადაწყვეტთ გამოიყენოთ WhatsApp-ი, როგორც უსაფრთხო მესინჯერის ოფცია, აუცილებლად გაეცანით ზემოთ მოცემულ სექციას მეტამონაცემების შესახებ. ასევე არსებობს რამდენიმე პარამეტრი, რომელთა სწორი კონფიგურაცია აუცილებელია. უმნიშვნელოვანესია, აუცილებლად გამორთოთ „ქლაუდის“ სათადარიგო ელემენტები ან, სულ მცირე, ჩართოთ WhatsApp-ის ახალი დაშიფრული სატრანსპორტო შრის სარეზერვო ასლების ფუნქცია 64 ციფრიანი ან უფრო გრძელი დაშიფვრის გასაღების - შემთხვევითი და უნიკალური კოდის გამოყენებით, რომელიც ინახება უსაფრთხო ადგილას (მაგალითად, თქვენი პაროლების მენეჯერში). ასევე აუცილებლად უჩვენეთ უსაფრთხოების შეტყობინებები და შეამოწმეთ უსაფრთხოების კოდები. ხსენებული პარამეტრების Android-ის ტელეფონებისათვის კონფიგურაციის მარტივი სახელმძღვანელო შეგიძლიათ იხ. აქ, iPhone-ებისათვის კი - აქ. **თუ თქვენი პერსონალი* და ისინი, ვისთანაც აწარმოებთ კომუნიკაციას* არამართებულად მოახდენენ ხსენებული ფუნქციების კონფიგურაციას, მაშინ არ უნდა მიიჩნიოთ WhatsApp-ი სენსიტიური კომუნიკაციის იმ კარგ საშუალებად, რომელსაც აბონენტური დაშიფვრა ესაჭიროება.** Signal-ი მაინც რჩება ხსენებული აბონენტური დაშიფვრით შეტყობინებების გაცვლის საუკეთესო საშუალებად გამომდინარე უსაფრთხოების მისი ნაგულისხმევი პარამეტრებიდან და მეტამონაცემების დაცვიდან.

რას იტყვით ტექსტურ შეტყობინებებზე?

ტექსტური შეტყობინებები ძირითადად მეტად დაუცველია (სტანდარტული SMS-ი დაუშიფრავია) და თავიდან უნდა იქნას აცილებული ყველაფრისათვის, რაც არ უნდა იყოს ცნობილი საზოგადოებისათვის. Apple-ის iPhone-iPhone შეტყობინებები (ცნობილი, როგორც iMessage-ები) კი დაშიფრულია აბონენტურად, მაგრამ თუ საუბარში ჩართულია არა-iPhone-ი, შეტყობინებები აღარაა უსაფრთხო. უსაფრთხოებისათვის ყველაზე კარგია **მოვერიდოთ ტექსტურ შეტყობინებებს შეტყობინებებს ყველაფერზე, რაც არის სენსიტიური, პირადი და კონფიდენციალური.**

რატომ არაა რეკომენდებული უსაფრთხო ჩატისათვის TELEGRAM, FACEBOOK MESSENGER ან VIBER?

ზოგიერთი სერვისი, როგორიცაა Facebook Messenger და Telegram, გვთავაზობს მხოლოდ აბონენტური დაშიფვრას, თუ თქვენ შეგნებულად (და მხოლოდ ერთი-ერთზე ჩატებისათვის) ჩართავთ მას, ასე რომ, ისინი არ წარმოადგენს კარგ არჩევანს სენსიტიური ან პირადი შეტყობინებების გასაცვლელად, განსაკუთრებით, ორგანიზაციისათვის. ნუ ენდობით ხსენებულ ინსტრუმენტებს, თუ გესაჭიროებათ აბონენტური დაშიფვრის გამოყენება, რადგან სრულიად მარტივია ნაგულისხმევი, ნაკლებად უსაფრთხო პარამეტრების შეცვლის დავიწყება. Viber-ი აცხადებს, რომ გვთავაზობს აბონენტურ დაშიფვრას, თუმცა, არ გადაუცია შესამოწმებლად საკუთარი პროგრამა უსაფრთხოების დამოუკიდებელი მკვლევარებისათვის. Telegram-ის პროგრამა ასევე არ გამხდარა ხელმისაწვდომი საჯარო აუდიტისათვის. შედეგად, მრავალი ექსპერტი შიშობს, რომ Viber-ის დაშიფვრა (ან Telegram-ის „საიდუმლო ჩეთი“) შესაძლოა არ აკმაყოფილებდეს სტანდარტს და, შესაბამისად, გამოუსადეგარი იყოს კომუნიკაციისათვის, რომელიც აბონენტურ დაშიფვრას საჭიროებს.

ჩვენი კოლეგები და კონტაქტები იყენებენ სხვა შეტყობინებების აპებს - როგორ დავარწმუნოთ ისინი ჩამოტვირთონ ახალი აპი ჩვენთან საკომუნიკაციოდ?

ხანდახან ადგილი აქვს არჩევანს უსაფრთხოებას და კომფორტს შორის, თუმცა, მცირედ მეტი ძალისხმევა ღირს სენსიტიური კომუნიკაციის დასაცავად. მოუყვანეთ კარგი მაგალითი თქვენს კონტაქტებს. თუ იძულებული ხართ გამოიყენოთ სხვა ნაკლებად უსაფრთხო სისტემები, კარგად გაიაზრეთ თუ რას ამბობთ. მოერიდეთ სენსიტიურ თემებზე დისკუსიას. ზოგიერთი ორგანიზაცია შესაძლოა იყენებდეს ერთ სისტემას საზოგადოდ და მეორეს ხელმძღვანელობასთან მეტად კონფიდენციალურ დისკუსიებზე ჩეთისათვის. რა თქმა უნდა, ყველაზე მარტივია, თუ ყველაფერი ყოველთვის ავტომატურად დაიშიფრება - არაფერია გასახსენებელი ან საფიქრალი.
საბედნიეროდ, აბონენტური დაშიფვრის აპები, როგორიცაა Signal-ი, სულ უფრო პოპულარული და მომხმარებელზე მორგებული ხდება - რომ არაფერი ვთქვათ იმაზე, რომ ისინი ლოკალიზებულია ათობით ენაზე გლობალური მოხმარებისათვის. თუ თქვენი პარტნიორები ან სხვა კონტაქტები საჭიროებენ დახმარებას კომუნიკაციის აბონენტური დაშიფვრის რეჟიმზე, მაგალითად Signal-ზე გადართვაში, გამოყავით დრო მათთან სასაუბროდ და აუხსენით რატომაა მნიშვნელოვანი თქვენი კომუნიკაციის სათანადოდ დაცვა. როცა ყველას ესმის მნიშვნელობა, ახალი აპის ჩამოტვირთვას რამდენიმე წუთი უნდა, ხოლო გამოყენებისას შეჩვევას რამდენიმე დღე შესაძლოა დასჭირდეს რაც არაა ძნელი საქმე.

არსებობს სხვა პარამეტრები აბონენტური დაშიფვრის აპებისათვის, რომელთა შესახებაც უნდა ვიცოდეთ?

აპში Signal-ი ასევე მნიშვნელოვანია უსაფრთხოების კოდების (რომლებსაც ისინი „უსაფრთხოების რიცხვებს“ (Safety Numbers-ს) უწოდებენ) შემოწმება. Signal-ში უსაფრთხოების რიცხვების სანახავად და შესამოწმებლად შეგიძლიათ გახსნათ თქვენი ჩეთი კონტაქტთან, დააჭიროთ მის სახელს თქვენი ეკრანის თავში და ჩამოხვიდეთ ქვემოთ „View Safety Number”-ზე დასაჭერად. თუ თქვენი უსაფრთხოების რიცხვი ემთხვევა თქვენს კონტაქტს, შეგიძლიათ მონიშნოთ ის, როგორც „შემოწმებული“ იგივე ეკრანზე. განსაკუთრებით მნიშვნელოვანია ყურადღება მიაქციოთ აღნიშნულ უსაფრთხოების რიცხვებს და შეამოწმოთ კონტაქტები, თუ მიიღეთ შეტყობინება ჩეთში, რომ თქვენი უსაფრთხოების რიცხვი მოცემულ კონტაქტთან შეიცვლა. თუ თქვენ ან პერსონალის სხვა წევრი საჭიროებთ დახმარებას ხსენებული პარამეტრების კონფიგურაციაში, Signal-ი თავად **გთავაზობთ სასარგებლო მითითებებს.** თუ იყენებთ Signal-ს, რომელიც ფართოდ განიხილება მომხმარებელზე მორგებულ საუკეთესო ოფციად შეტყობინებების უსაფრთხოდ მიმოცვლისათვის და ერთი-ერთზე ზარებისათვის, აუცილებლად **დააყენეთ ძლიერი პინი.** გამოიყენეთ, სულ მცირე, ექვსი ციფრი და არა რაიმე ადვილად გამოსაცნობი, როგორიცაა თქვენი დაბადების თარიღი. დამატებითი რჩევებისათვის, თუ როგორ მოვახდინოთ **Signal-ის** და **WhatsApp-ის** სწორი კონფიგურაცია, შეგიძლიათ გაეცნოთ **ინსტრუმენტების სახელმძღვანელოებს**, რომელიც ორივესათვის შეიმუშავა EFF-მა „თვალთვალისაგან თავდაცვის სახელმძღვანელოს“ ფარგლებში.

ჩეთის აპების გამოყენება რეალურ სამყაროში

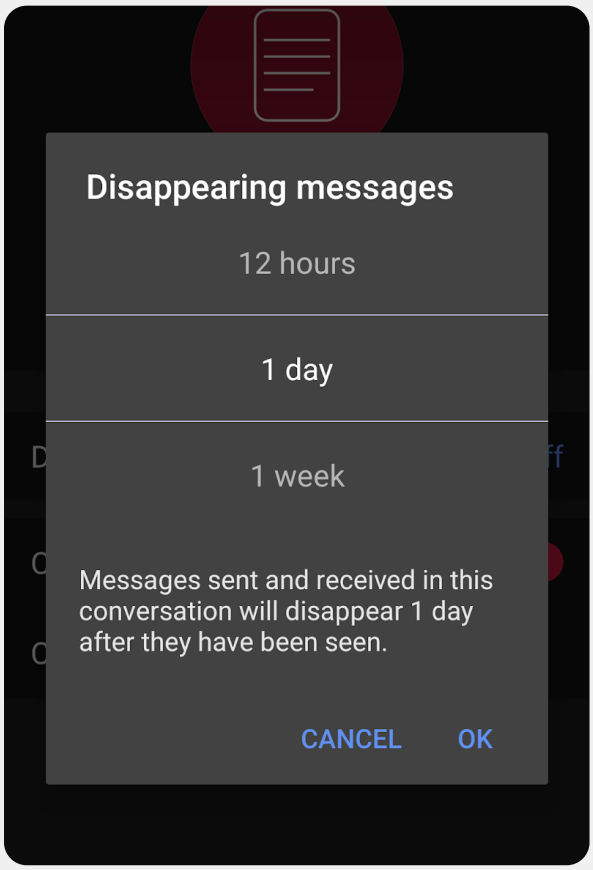
ტელეფონის დაკარგვის, ქურდობის ან კონფისკაციის შემთხვევაში ზიანის შეზღუდვის მიზნით საუკეთესო მეთოდია იმ შეტყობინებების ისტორიის მინიმუმამდე დაყვანა, რომლებიც ინახება თქვენს ტელეფონში. ამის ერთი მარტივი გზაა ჩართოთ „**disappearing messages**“-ი თქვენი ორგანიზაციის ჯგუფური ჩეთებისათვის და წაახალისოთ პერსონალი ასევე გააკეთოს იგივე საკუთარი პირადი ჩეთებისათვის.

Signal-ში და სხვა პოპულარულ შეტყობინებების აპლიკაციებში შეგიძლიათ დააყენოთ დრო შეტყობინებების გასაქრობად - წაკითხვიდან წუთების ან საათების კონკრეტული რიცხვი. ხსენებული პარამეტრი შესაძლოა მორგებული იქნა გამომდინარე ინდივიდუალური ან ჯგუფური ჩეთიდან. ჩვენი უმრავლესობისათვის გასაქრობი ფანჯრისათვის ერთი კვირის დაყენება უამრავ დროს გაძლევთ ყველაფრის საქმის კურსში ყოფნისათვის და ამავდროულად, არ შეინახავთ შეტყობინებებს, რომლებიც არასდროს დაგჭირდებათ, – მაგრამ რომლებიც შესაძლოა გამოყენებული იქნას თქვენს წინააღმდეგ მომავალში. გახსოვდეთ, შეუძლებელია იმის მოპარვა, რაც არ გაქვთ.

Signal-ში გასაქრობი შეტყობინებების ჩასართავად გახსენით ჩეთი, დააჭირეთ პირის/ჯგუფის სახელს, რომელთანაც გაქვთ ჩეთი, დააჭირეთ გასაქრობ შეტყობინებებს, აირჩიეთ დრო და დააჭირეთ ok-ს. მსგავსი პარამეტრი არსებობს WhatsApp-შიც.

უფრო სერიოზულ სიტუაციებში, სადაც არსებობს შეტყობინების დაუყონებლივ წაშლის საჭიროება, რადგან შესაძლოა ვინმეს ტელეფონი მოიპარეს ან გაუგზავნეთ შეტყობინება სხვა პირს, აღსანიშნავია, რომ Signal-ი გაძლევთ საშუალებას წაშალოთ შეტყობინება ჯგუფის ან ცალკეული პირისადმი ყველას ტელეფონიდან მისი გაგზავნიდან სამი საათის განმავლობაში მისი უბრალოდ ჩეთიდან წაშლით. Telegram-ი კვლავაც პოპულარულია მრავალ ქვეყანაში მიუხედავად მისი დაშიფვრის შეზღუდვებისა მსგავსი ფუნქციის გამო, რომელიც საშუალებას აძლევს მომხმარებელს წაშალოს შეტყობინებები ყველა აპარატში შეზღუდვის გარეშე.

ამგვარად, თუ თქვენი ორგანიზაცია შეშფოთებულია პერსონალის უსაფრთხოების გამო იმ კომუნიკაციის შედეგად, რომელიც შესაძლოა ჩანდეს მათ ტელეფონებში, მაშინ მოკლე ტაიმერით გასაქრობი შეტყობინებების გამოყენება სავარაუდოდ უმარტივესი და ძალიან მდგრადი ოფციაა.



რას იტყვით უფრო ფართო ჯგუფის ვიდეო-ზარებზე? არსებობს აბონენტური დაშიფვრის ოფციები?

დისტანციური სამსახურის მატებასთან ერთად მნიშვნელოვანია გვქონდეს უსაფრთხოების ოფცია თქვენი ორგანიზაციის დიდი ჯგუფის ვიდეო-ზარებისათვის. სამწუხაროდ, დღეისათვის არ არსებობს იმ ოფციების დიდი არჩევანი, რომელიც დააკმაყოფილებდა ყველაფერს: მომხმარებელზე მორგებული, დამსწრეთა დიდი რიცხვის მხარდაჭერა და კოლაბორაციის ფუნქციები, ასევე, აბონენტური დაშიფვრის უპირობო ჩართვა.

40 ადამიანამდე ჯგუფებისათვის, Signal-ი მაქსიმალურად რეკომენდებული აბონენტური დაშიფვრის ოფციაა. ჯგუფურ ვიდეო-ზარებში Signal-ში შესაძლოა ჩაერთოს როგორც სმარტფონი, ისე კომპიუტერი Signal-ის დესკტოპის აპით, რომელიც იძლევა ეკრანის გაზიარების შესაძლებლობას. თუმცა, გახსოვდეთ, რომ Signal-ის ჯგუფში შესაძლოა მხოლოდ თქვენი ისეთი კონტაქტების დამატება, რომლებიც უკვე იყენებენ Signal-ს.

თუ ეძებთ სხვა ოფციებს, ერთი პლატფორმა, რომელმაც ახლახანს დაამატა აბონენტური დაშიფვრის პარამეტრი, არის **Jitsi Meet-ი**. Jitsi Meet-ი წარმოადგენს ინტერნეტით მომუშავე აუდიო და ვიდეო კონფერენციის გადაწყვეტას, რომელსაც შეუძლია იმუშაოს დიდ აუდიტორიაზე (100-მდე ადამიანი) და არ საჭიროებს რაიმე აპის ჩამოტვირთვას ან სპეციალურ პროგრამულ უზრუნველყოფას. აღსანიშნავია, რომ თუ იყენებთ აღნიშნულ ფუნქციას დიდი ჯგუფებისათვის (15-20 ადამიანზე მეტი), ზარის ხარისხი შესაძლოა შემცირდეს. Jitsi Meet-ში შეხვედრის მოსაწყობად შეგიძლიათ გადახვიდეთ **meet.jit.si-ზე**, ჩაწეროთ შეხვედრის კოდი და გაუზიაროთ ხსენებული ბმული (უსაფრთხო არხით, როგორიცაა Signal-ი) თქვენთვის სასურველ მონაწილეებს. აბონენტური დაშიფვრის გამოსაყენებლად იხ. Jitsi-ის მიერ შემუშავებული ეს **მითითებები**. აღსანიშნავია, რომ ყველა ინდივიდუალურმა მომხმარებელმა თავად უნდა აამოქმედოს აბონენტური დაშიფვრა, რათა ის ამუშავდეს. Jitsi-ის გამოყენებისას უეჭველად შეადგინეთ ოთახის შემთხვევითი დასახელებები და გამოიყენეთ ძლიერი პაროლები თქვენი ზარების დასაცავად.

თუ აღნიშნული ოფცია გამოუსადეგარია თქვენი ორგანიზაციისათვის, შეგიძლიათ გამოიყენოთ პოპულარული კომერციული ოფცია, როგორიცაა Webex-ი ან Zoom-ი მოქმედი აბონენტური დაშიფვრით. Webex-მა დიდი ხანია შემოიღო აბონენტური დაშიფვრა; თუმცა, ხსენებული ოფცია არაა ჩართული უპირობოდ და საჭიროებს მონაწილეების მიერ Webex-ის ჩამოტვირთვას შეხვედრაში ჩართვისათვის. Webex-ის თქვენს პროფილზე აბონენტური დაშიფვრის ოფციის მისაღებად თქვენ უნდა გახსნათ Webex-ის მხარდაჭერის კეისი და შეასრულოთ **ეს მითითებები**, რათა უზრუნველყოთ აბონენტური დაშიფვრის კონფიგურაცია. აბონენტური დაშიფვრა უნდა ჩართოს მხოლოდ შეხვედრის ორგანიზატორმა. ასეთ შემთხვევაში მთელი შეხვედრა იქნება აბონენტურად დაშიფრული. თუ Webex-ი გამოიყენება უსაფრთხო ჯგუფური შეხვედრების და კონფერენციებისათვის, ასევე უეჭველად შექმენით ძლიერი პაროლები თქვენი ზარებისათვის.

პრესაში ნეგატიური გამოხმაურებიდან თვეების შემდეგ Zoom-მა შეიმუშავა **აბონენტური დაშიფვრის ოფცია** საკუთარი ზარებისათვის. თუმცა, აღნიშნული ოფცია არა ჩართული უპირობოდ, საჭიროებს, რომ ზარის ინიციატორმა მიაბას საკუთარი პროფილი ტელეფონის ნომერს და ის ამუშავდება მხოლოდ მაშინ, თუ ყველა მონაწილე ჩაერთვება Zoom-ის დესკტოპით ან მობილური აპლიკაციით ნაცვლად ნომრის აკრეფისა. რამდენადაც მარტივია, შემთხვევით არასწორი კონფიგურაციით დააყენოთ ხსენებული პარამეტრები, იმდენად არასასურველია, დაეყრდნოთ Zoom-ს, როგორც აბონენტური დაშიფვრის ოფციას. თუმცა, თუ აბონენტური დაშიფვრა საჭიროა და Zoom-ი თქვენი ერთადერთი ალტერნატივაა, შეგიძლიათ შეასრულოთ Zoom-ის **მითითებები** მისი კონფიგურაციისათვის. უბრალოდ აუცილებლად შეამოწმეთ ნებისმიერი ზარი დაწყებამდე, რათა უზრუნველყოთ მისი დანამდვილებით აბონენტური დაშიფვრა Zoom-ის ეკრანის ზედა მარცხენა კუთხეში მწვანე საკეტზე დაწკაპუნებით და „აბონენტურის“ გამოჩენით დაშიფვრის ფუნქციის გასწვრივ. ასევე უნდა შევადგინოთ ძლიერი პაროლი Zoom-ში ნებისმიერი შეხვედრისათვის.

გარდა ზემოხსენებული ინსტრუმენტების, Frontline Defenders-ის მიერ შემუშავებული **ეს დიაგრამა** უჩვენებს ზოგიერთ ვიდეო ზარის და კონფერენციის ოფციებს, რომლებიც, გამომდინარე თქვენის რისკის კონტექსტიდან, შესაძლოა მნიშვნელოვანი იყოს თქვენი ორგანიზაციისათვის.

თუმცა, უნდა აღინიშნოს, რომ ზემოხსენებული ინსტრუმენტების კონკრეტული პოპულარული ფუნქციები მუშაობს მხოლოდ სატრანსპორტო შრის დაშიფვრასთან ერთად. მაგალითად, აბონენტური დაშიფვრის ჩართვა Zoom-ში თიშავს ჯგუფური დისკუსიის ოთახებს, კენჭისყრის შესაძლებლობებს და „ქლაუდზე“ ჩაწერას. Jitsi Meet-ში ჯგუფური დისკუსიის ოთახებს შეუძლია გამორთოს აბონენტური დაშიფვრის ფუნქცია, რაც იწვევს უსაფრთხოების უნებლიე შესუსტებას.

რა ხდება, თუ რეალურად არ გვჭირდება აბონენტური დაშიფვრა მთელი ჩვენი კომუნიკაციისათვის?

თუ აბონენტური დაშიფვრა არაა საჭირო თქვენი ორგანიზაციის მთელი კომუნიკაციისათვის გამომდინარე თქვენი რისკების შეფასებიდან, შეგიძლიათ გამოიყენოთ სატრანსპორტო შრის დაშიფვრით დაცული აპლიკაციები. გახსოვდეთ, რომ დაშიფვრის მოცემული ტიპი საჭიროებს, რომ ენდობოდეთ სერვისის მიმწოდებელს, როგორიცაა Google-ი Gmail-თვის, Microsoft-ი Outlook/Exchange-თვის ან Facebook-ი Messenger-თვის, რადგან მათ (და ყველას, ვისთვისაც ინფორმაციის გაზიარება შესაძლოა აიძულონ მათ) შეუძლიათ თქვენი კომუნიკაციის დანახვა/მოსმენა. კიდევ ერთხელ, საუკეთესო ოფციები დამოკიდებული იქნება თქვენს წინაშე არსებულ საფრთხეზე (მაგალითად, თუ არ ენდობით Google-ს ან თუ აშშ-ის მთავრობა თქვენი მეტოქეა, მაშინ Gmail-ი არაა კარგი ოფცია), თუმცა, რამდენიმე პოპულარული და ზოგადად სანდო ოფცია მოიცავს:

ელ-ფოსტა	• **Gmail-ი (Google Workspace-ით)** • **Outlook-ი (Office 365-ით)** • ნუ იქნებით თქვენი საკუთარი Microsoft Exchange-ის სერვერი თქვენი ორგანიზაციის ელ-ფოსტისათვის. **თუ ახლა ასრულებთ ამ როლს, უნდა გადახვიდეთ Office 365-ზე.**
ტექსტური მესინჯერი (ინდივიდუალური ან ჯგუფური)	• **Google Hangouts-ი** • **Slack-ი** • **Microsoft Teams-ი** • **Mattermost-ი** • **Line-ი** • **KaKao Talk-ი** • **Telegram-ი**
ჯგუფური კონფერენციები, აუდიო და ვიდეო ზარები	• **Jitsi Meet-ი** • **Google Meet-ი** • **Microsoft Teams-ი** • **Webex-ი** • **GotoMeeting-ი** • **Zoom-ი**
ფაილების გაზიარება	• **Google Drive-ი** • **Microsoft Sharepoint-ი** • **Dropbox-ი** • **Slack-ი** • **Microsoft Teams-ი**

შენიშვნა ფაილების გაზიარების შესახებ

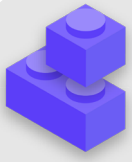
გარდა შეტყობინებების უსაფრთხო გაზიარებისა, ფაილების უსაფრთხო გაზიარება სავარაუდოდ წარმოადგენს თქვენი ორგანიზაციის უსაფრთხოების გეგმის მნიშვნელოვან ნაწილს. ფაილების გაზიარების ოფციების უმეტესობა ჩაშენებული შეტყობინებების გაგზავნის აპლიკაციებში ან სერვისებში, რომლებსაც შესაძლოა უკვე იყენებთ. მაგალითად, ფაილების გაზიარება Signal-ის საშუალებით მშვენიერი ოფციაა, თუ გესაჭიროებათ აბონენტური დაშიფვრა. თუ სატრანსპორტო შრის დაშიფვრა საკმარისია, Google Drive-ის ან Microsoft SharePoint-ის გამოყენება შესაძლოა კარგი არჩევანი იყოს თქვენი ორგანიზაციისათვის. უბრალოდ უეჭველად მოახდინეთ გაზიარების პარამეტრების სწორად კონფიგურაცია ისე, რომ კონკრეტულ დოკუმენტზე ან საქაღალდეზე წვდომა მხოლოდ შესაფერის ხალხს გააჩნდეს და უზრუნველყავით, რომ ხსენებული სერვისები დაკავშირებული იყოს პერსონალის ორგანიზაციული (და არა პირადი) ელ-ფოსტის პროფილებთან. თუ შეგიძლიათ, აკრძალეთ სენსიტიური ფაილების გაზიარება ელ-ფოსტის დანართების სახით ან ფიზიკურად USB-ების საშუალებით. USB-ების მსგავსი მოწყობილობების გამოყენება თქვენი ორგანიზაციის ფარგლებში მნიშვნელოვნად ზრდის საზიანო პროგრამის თუ ქურდობის ალბათობას, ხოლო ელ-ფოსტის დანართებზე თუ დანართის სხვა ფორმებზე დაყრდნობა ასუსტებს თქვენი ორგანიზაციის ფიშინგური შეტევებისაგან დაცვის სქემას.



ფაილების გაზიარების ორგანიზაციული ალტერნატივები

თუ ეძებთ ფაილების გაზიარების უსაფრთხო ოფციას თქვენი ორგანიზაციისათვის, რომელიც არაა უშუალოდ მიბმული შეტყობინებების გაგზავნის პლატფორმაზე (ან შესაძლოა დაწესებული გაქვთ ფაილის ზომის ლიმიტი დიდი დოკუმენტების გაზიარებისას), დაფიქრდით OnionShare-ზე. **OnionShare-ი** წარმოადგენს ღია კოდის მქონე ინსტრუმენტს, რომელიც საშუალებას გაძლევთ უსაფრთხოდ და ანონიმურად გააგზავნოთ გააგზავნოთ ნებისმიერი ზომის ფაილი. ის მუშაობს, როცა გამგზავნს ჩამოტვირთული აქვს აპი OnionShare-ი (ხელმისაწვდომი Mac-ის, Windows-ის და Linux-ის კომპიუტერებისათვის), ატვირთავს ფაილს (ფაილებს), რომლის გაზიარებაც სურს და შეიქმნება უნიკალური ბმული. აღნიშნული ბმული, რომელიც შესაძლოა გამოყენებული იქნას მხოლოდ Tor Browser-ში, შესაძლოა გაზიარებული იქნას შეტყობინებების ნებისმიერი უსაფრთხო არხით (მაგალითად, Signal-ი) სასურველ მიმღებთან. შემდეგ მიმღებს შეუძლია გახსნას ბმული Tor Browser-ში და ჩამოტვირთოს ფაილი (ფაილები) საკუთარ კომპიუტერში. გახსოვდეთ, რომ ფაილები დაცულია მხოლოდ იმდენად, რამდენადაც მეთოდი, რომლითაც აზიარებთ ბმულს. Tor-ი უფრო დეტალურად განიმარტება სახელმძღვანელოს მომდევნო სექციაში „მნიშვნელოვანია“, თუმცა, თქვენს ორგანიზაციაში ფაილების გაზიარების მიზნით, გახსოვდეთ OnionShare-ი, როგორც USB-ებით ოფისში დიდი ფაილების უფრო უსაფრთხო გაზიარების ალტერნატივა, თუ არ გყავთ სანდო Cloud-ის პროვაიდერი.

თუ თქვენს ორგანიზაციას უკვე შეძენილი აქვს პაროლების დისპეტჩერი, წინამდებარე სახელმძღვანელოს პაროლების სექციაში აღწერილის შესაბამისად, და ირჩევს Bitwarden-ის პრემიუმ ან ჯგუფურ პროფილს, **Bitwarden Send-ის** ფუნქცია წარმოადგენს კიდევ ერთ ოფციას ფაილების უსაფრთხო გაზიარებისათვის. აღნიშნული ფუნქცია საშუალებას აძლევს მომხმარებელს შექმნას უსაფრთხო ბმულები გაზიარებულ უსაფრთხო ფაილებზე ნებისმიერი შეტყობინებების უსაფრთხო არხით (როგორიცაა Signal-ი). ფაილის ზომა შეზღუდულია 100Mb-ით, თუმცა, Bitwarden Send-ი საშუალებას გაძლევთ მიაბათ ბმულებს განმარტებითი ინფორმაცია, დაიცვათ გაზიარებულ ფაილებზე წვდომა პაროლით და შეზღუდოთ თქვენი ბმულის გახსნების რიცხვი.



უსაფრთხო კომუნიკაცია და მონაცემების გაზიარება

- **მოითხოვეთ სანდო აბონენტური დაშიფვრის მქონე შეტყობინებების სერვისის გამოყენება თქვენი ორგანიზაციის სენსიტიური კომუნიკაციისათვის (იდეალურ შემთხვევაში კი - მთელი კომუნიკაციისათვის).**
  - დაუთმეთ დრო პერსონალის და პარტნიორებისათვის იმის განმარტებას, თუ რატომაა უსაფრთხო კომუნიკაცია ამდენად მნიშვნელოვანი; ეს მნიშვნელოვანი; ეს უზრუნველჰყოფს თქვენი გეგმის წარმატებას.
- **დაადგინეთ პოლიტიკის ფარგლებში, თუ რამდენ ხანს შეინახავთ შეტყობინებებს და როდის/თუ გამოიყენებს ორგანიზაცია კომუნიკაციის „გაქრობის“ ფუნქციას.**
- **უზრუნველყავით მართებული პარამეტრების დაყენება უსაფრთხო კომუნიკაციის აპებში, მათ შორის:**
  - უზრუნველყავით, რომ მთელმა პერსონალმა მიაქციოს ყურდღება უსაფრთხოების შეტყობინებებს და, WhatsApp-ის გამოყენების შემთხვევაში, არ აწარმოოს ჩეთების ასლების შენახვა.
  - იმ აპის გამოყენების შემთხვევაში, სადაც აბონენტური დაშიფვრა არაა ჩართული უპირობოდ (მაგ. Zoom-ი ან Webex-ი), უზრუნველყავით, რომ შესაფერის მომხმარებელს ჩართული ჰქონდეს შესაბამისი პარამეტრები ნებისმიერი ზარის ან შეხვედრის დაწყებამდე.
- **თქვენი ორგანიზაციისათვის გამოიყენეთ ქლაუდზე დაფუძნებული ელ-ფოსტის სერვისები, როგორიცაა Office 365-ი ან Gmail-ი.**
  - ნუ ეცდებით იყოთ ჰოსტი თქვენი საკუთარი ელ-ფოსტის სერვერისათვის.
  - ნუ მისცემთ საშუალებას პერსონალს გამოიყენოს ელ-ფოსტის პირადი პროფილები სამსახურისათვის.
- **ხშირად შეახსენეთ ორგანიზაციას ჯგუფურ შეტყობინებებთან და მეტამონაცემებთან დაკავშირებული უსაფრთხოების აღიარებული მეთოდიკა.**
  - იცოდეთ ვინ არის ჩართული ჯგუფურ შეტყობინებებში, ჩეთებში და ელ-ფოსტით მიმოწერაში.

მონაცემების უსაფრთხოდ შენახვა

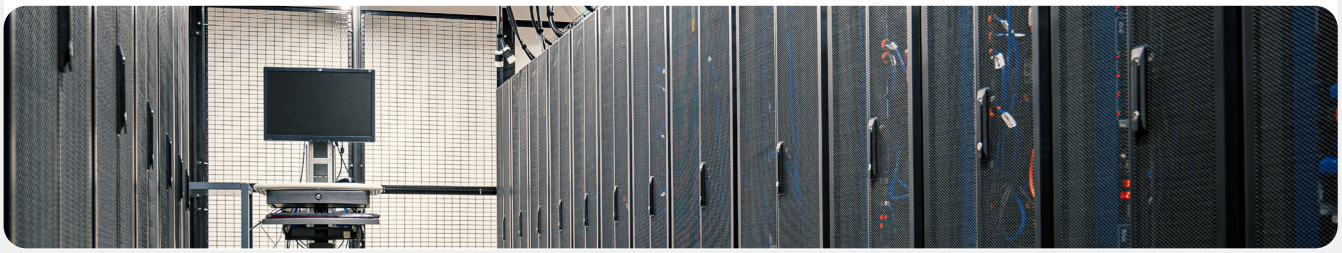
სამოქალაქო საზოგადოებრივი ორგანიზაციების უმეტესობისათვის, ერთ-ერთი უმნიშვნელოვანესი გადაწყვეტილებაა, სად შეინახოს საკუთარი მონაცემები.

„უფრო უსაფრთხოა“ მონაცემების შენახვა პერსონალის კომპიუტერებში, ადგილობრივ სერვერზე, გარე შესანახ მოწყობილობებზე თუ ქლაუდზე? სიტუაციების 99 პროცენტში უმარტივესი და მაქსიმალურად უსაფრთხო ოფციაა მონაცემთა შენახვა სანდო დისტანციურ (ქლაუდ-) საცავებში. ალბათ ყველაზე ტიპური მაგალითები მოიცავს Microsoft 365-ს და Google Drive-ს. დისტანციური საცავის ყოვლისმომცველი გეგმის გარეშე სავარაუდოა, რომ თქვენი ორგანიზაციის მონაცემები ინახება სხვადასხვა ადგილებში - მათ შორის, პერსონალის კომპიუტერებში, გარე მყარ დისკებზე და რამდენიმე ადგილობრივ სერვერზეც კი. ყველა ამ მოწყობილობაში მონაცემთა დაცვა კი შესაძლებელია, მაგრამ მეტად რთულია ამის წარმატებულად გაკეთება დიდი ხარჯის და IT-ის პერსონალის დაქირავების გარეშე.

თქვენი მონაცემების შესანახად სერვისის ან ინსტრუმენტის შერჩევისას, უზრუნველყავით, რომ ენდობოდეთ მათ უკან მდგომ კომპანიას ან ჯგუფს. გუგლით ძიებას და ციფრული უსაფრთხოების ექსპერტებთან შემოწმებას შესაძლოა დიდი გავლენა ჰქონდეს თქვენს მიერ პოტენციური ტექ. მომწოდებლის სანდოობის დადგენაზე. რამდენიმე კითხვა, რომელიც უნდა გახსოვდეთ, მოიცავს: ხომ არ ყიდიან ან აზიარებენ თქვენს პირად მონაცემებს? გააჩნიათ მათ შესაფერისი უსაფრთხოების რესურსები ან პერსონალი? უზრუნველყოფენ ისინი უსაფრთხოების ფუნქციებს (მაგალითად, 2Fa-ი) თქვენი პროფილის დაცვაში თქვენს დასახმარებლად?

მონაცემთა შენახვა და სამოქალაქო საზოგადობა

ქლაუდზე მომუშავე ხელმისაწვდომი (ხანდახან უფასო) მონაცემთა საცავის გამოჩენამ გაამარტივა (და უფრო უსაფრთხო გახადა) ცხოვრება არაერთი რესურსებში შეზღუდული სამოქალაქო საზოგადოებრივი ორგანიზაციისათვის. სამწუხაროდ, ბევრი ჯერაც ცდილობს შეასრულოს ჰოსტის ფუნქცია საკუთარი სერვერებისათვის მეტ-ნაკლებად შეზღუდული IT-ბიუჯეტით, პერსონალით და მხარდაჭერით. 2021 წ.მარტში აღნიშნული ორგანიზაციული ინფრასტრუქტურის საფრთხე რეალური გახდა ათობით ათასი ორგანიზაციისათვის მთელს მსოფლიოში, როცა ჩინეთის მთავრობასთან დაკავშირებულმა ბოროტმოქმედთა ჯგუფმა Hafnium-მა მოაწყო კატასტროფა გლობალური კიბერუსაფრთხოებისათვის, წამოიწყო რა შეტევა თვით-ჰოსტ Microsoft Exchange-ის სერვერებზე. შეტევისას გატეხილი იქნა ადგილობრივი სერვერები, რამაც საშუალება მისცა ჰაკერებს მიეღოთ წვდომა ელ-ფოსტის ორგანიზაციულ პროფილებზე, მოეხდინათ დამატებითი საზიანო პროგრამის ინსტალაცია მსხვერპლის სერვერებზე და ჩართულ სისტემებში და საბოლოოდ მოეპოვებინათ სენსიტიური მონაცემები. ჰაკერობის გასაჯაროების შემდეგ, სანამ Microsoft-ი გამოაქვეყნებდა განახლებას და მითითებებს პოტენციური მიმტაცებლების იდენტიფიცირების და მოცილების შესახებ, მრავალი ორგანიზაციის IT-მ ვერ უზრუნველყო ხსენებული განახლების ოპერატიულად გამოყენება, რამაც ისინი დაუცველი დატოვა ხანგრძლივი დროით. აღნიშნული გლობალური ჰაკერობის ფარგლები და გავლენა გვიჩვენებს საფრთხეს იმ პარტიებისათვის. რომლებიც თავად ასრულებენ ჰოსტის როლს საკუთარი ელ-ფოსტის სერვერებისა და სხვა ტიპის სენსიტიური მონაცემებისთვის კიბერუსაფრთხოების პერსონალში მნიშვნელოვანი ინვესტიციების.



ქლაუდ-საცავის უპირატესობები

თქვენი კომპიუტერის საზიანო პროგრამისაგან და ფიზიკური ქურდობისაგან დასაცავად თქვენს მიერ ყველა მართებული ზომის მიღების შემთხვევაშიც კი შეუპოვარმა მეტოქემ მაინც შესაძლოა გატეხოს თქვენი კომპიუტერი ან ადგილობრივი სერვერი. მათთვის გაცილებით რთულია გატეხონ Google-ის ან Microsoft-ის უსაფრთხოების დაცვის სისტემები. კარგ ქლაუდ-საცავ კომპანიებს გააჩნია შეუდარებელი უსაფრთხოების რესურსები და მყარი ბიზნეს-სტიმული უზრუნველყოს საკუთარი მომხმარებლის უსაფრთხოება. მოკლედ: სანდო ქლაუდ-საცავის სტრატეგია გაცილებით მარტივია სარეალიზაციოდ და უსაფრთხოების დასაცავად დროის ხანგრძლივი პერიოდის განმავლობაში. ამგვარად, საკუთარი სერვერის უსაფრთხოების მცდელობაზე ნერვიულობის ნაცვლად შეგიძლიათ კონცენტრაცია მოახდინოთ რიგ უფრო მარტივ ამოცანაზე. თქვენი ინფორმაციის მასივის ქლაუდზე შენახვა გეხმარებათ რიგ საყოველთაო რისკებთან მიმართებაში. დარჩა ვინმეს კომპიუტერი რესტორანში ან ტელეფონი ავტობუსში? გადააბრუნა ბავშვმა ჭიქა წვენი თქვენს კლავიატურაზე და გააფუჭა თქვენი მოწყობილობა? გაუჩნდა თანამშრომელს საზიანო პროგრამა და საჭიროა მისი კომპიუტერის წაშლა და ფორმატირება? თუ დოკუმენტების და მონაცემების უმეტესობა ქლაუდზე ინახება, მარტივია მათი ხელახლა სინქრონიზაცია გაწმენდილ ან სრულიად ახალ კომპიუტერზე. ასევე, თუ საზიანო პროგრამა აღწევს კომპიუტერში ან თუ ქურდი მოახდენს მყარი დისკის სკანირებას, არაფერი იქნება მოსაპარი, თუ დოკუმენტების უმეტესობაზე წვდომა ბრაუზერით ხდება.

ქლაუდ-საცავის რომელი პროვაიდერი უნდა ავირჩიოთ?

ორი ყველაზე პოპულარული ქლაუდ-საცავია Google Workspace-ი (ადრე GSuite-ი) და Microsoft 365-ი. თუ თქვენ და თქვენი პერსონალი უკვე იყენებთ Gmail-ს, თქვენი ორგანიზაციის Google Workspace-ის აბონენტად რეგისტრაცია და მონაცემების შენახვა Google Drive-ში მისი საკუთარი აპლიკაციებით Google Docs-ი, Sheets-ი და Slides-ი ტექსტის რედაქტირების, ცხრილების და პრეზენტაციების მოსამზადებლად სრულიად გონივრულია. ანალოგიურად, თუ ხართ ორგანიზაცია, რომელიც დამოკიდებულია Excel-ზე და Word-ზე, მარტივი არჩევანია გახდეთ Microsoft 365-ის გამომწერი, რომელიც თქვენს ორგანიზაციას ანიჭებს წვდომას Outlook-ზე ელ-ფოსტისათვის და Microsoft Word-ის, Excel-ის, Powerpoint-ის და Teams-ი ლიცენზირებულ ვერსიებზე. მიუხედავად თქვენს მიერ პროვიდერის არჩევანისა, მონაცემების უსაფრთხოდ შენახვა ქლაუდზე საჭიროებს გაზიარების აღიარებული პარამეტრების რეალიზაციას და პერსონალის ტრენინგს, რათა მას ესმოდეს, თუ როგორ და როდის გააზიაროს (და არ გააზიაროს) საქაღალდეები და დოკუმენტები. ზოგადად, თქვენს ქლაუდ-საცავში უნდა გააკეთოთ საქაღალდეები, რაც ზღუდავს წვდომას მხოლოდ პერსონალით, რომელსაც ის ესაჭიროება კონკრეტულ ფაილებზე წვდომისათვის. რეგულარულად შეამოწმეთ თქვენი სისტემა, რათა დარწუმდეთ, რომ „ზედმეტად“ არ აზიარებთ რომელიმე ფაილს (როგორიცაა უნივერსალური ბმულის გაზიარების ჩართვა ფაილებისათვის, რომლებიც ნაცვლად ამისა შეზღუდული უნდა იყოს მხოლოდ რამდენიმე ადამიანით).

რა ხდება, თუ არ ვენდობით Google-ს ან Microsoft-ს ან ქლაუდ-საცავის სხვა პროვაიდერებს?

თუ რომელიმე თქვენს მეტოქეს (მაგალითად, უცხოური ან ადგილობრივი მთავრობა) შეუძლია კანონიერად აიძულოს Google-ი ან Microsoft-ი (ან ქლაუდ-საცავის რომელიმე სხვა პროვაიდერი) გადასცეს მონაცემები, მაშინ შესაძლოა აზრს მოკლებული იყოს მათი მონაცემების საცავად არჩევა. ხსენებული რისკი შესაძლოა უფრო მაღალი იყოს, თუ თქვენი მეტოქე, მაგალითად, შეერთებული შტატების მთავრობაა, თუმცა, გაცილებით დაბალია, თუ თქვენი მეტოქე ავტორიტარული რეჟიმია. გახსოვდეთ, რომ როგორც Google-ს, ისე Microsoft-ს გააჩნია პოლიტიკა მონაცემების მხოლოდ მაშინ გადაცემის შესახებ, როცა ასე მოქცევა კანონით ევალება და აღიარებს, რომ თქვენი ორგანიზაცია შესაძლოა თავად იყოს მოწყვლადი თქვენი საკუთარი მთავრობის იგივე ხასიათის კანონიერი მოთხოვნების მიმართ, თუ ახდენს მონაცემების ჰოსტინგს ადგილობრივად. სიტუაციებში, როცა Google-ის ან Microsoft-ის ქლაუდ-საცავი აზრსაა მოკლებული თქვენი ორგანიზაციისათვის, გასათვალისწინებელი ალტერნატივაა Keybase-ი. Keybase-ის ფუნქცია „teams“-ი საშუალებას აძლევს თქვენს ორგანიზაციას გააზიაროს ფაილები და შეტყობინებების აბონენტური დაშიფვრის გამოყენებით უსაფრთხო ქლაუდ-გარემოში მესამე მხარის პროვაიდერის ნდობის გარეშე. შედეგად, ის შესაძლოა დოკუმენტების და ფაილების ორგანიზაციაში უსაფრთხოდ შენახვის კარგი ოფცია იყოს. თუმცა, Keybase-ი ნაკლებად ცნობილია მომხმარებლის უმრავლესობისათვის, ამდენად, იცოდეთ, რომ ხსენებული ინსტრუმენტის მიღება სავარაუდოდ მეტ ტრენინგს და ძალისხმევას მოითხოვს, ვიდრე სხვა ზემოხსენებული გადაწყვეტები. ამგვარად, თუ გადაწყვეტთ იმოქმედოთ დამოუკიდებლად და არ გამოიყენოთ ქლაუდ-საცავი, მნიშვნელოვანია, რომ დააბანდოთ დრო და რესურსები თქვენი მოწყობილობების ციფრული დაცვის გაძლიერებაში და უზრუნველყოთ ყველა ადგილობრივი სერვერის მართებულად კონფიგურაცია, დაშიფვრა და ფიზიკური უსაფრთხოება. შეგიძლიათ ეკონომია გააკეთოთ ყოველთვიური გამოწერის საფასურზე, თუმცა, ეს თქვენს ორგანიზაციას პერსონალის დროდ და რესურსებად, ასევე, შეტევებისადმი მეტ მოწყვლადობად დაუჯდება.

მონაცემების დუბლირება

მიუხედავად იმისა ინახავს თუ არა თქვენი ორგანიზაცია მონაცემებს ფიზიკურ მოწყობილებებში თუ ქლაუდზე, მნიშვნელოვანია სარეზერვო ასლის ფლობა. გახსოვდეთ, რომ თუ ენდობით შენახვას ფიზიკურ მოწყობილობაში, საკმაოდ მარტივია თქვენს მონაცემებზე წვდომის დაკარგვა. შესაძლოა ყავა დაგექცეთ თქვენს კომპიუტერზე და გაანადგუროთ მყარი დისკი. პერსონალის კომპიუტერებზე შესაძლოა მოხდეს ჰაკერული შეტევა და ყველა ადგილობრივ ფაილი შესაძლოა ბლოკირებული იქნას გამომძალველი პროგრამით.

ვინმემ შესაძლოა დაკარგოს მოწყობილობა მატარებელში ან ის შესაძლოა მოიპაროს მის პორტფელთან ერთად. ზემოხსენებულის თანახმად, ესაა კიდევ ერთი მიზეზი იმისა, თუ რატომ შესაძლოა იყოს სასარგებლო ქლაუდ-საცავის გამოყენება, რადგან ის არაა დაკავშირებული კონკრეტულ მოწყობილობასთან, რომელიც შესაძლოა დავირუსდეს, დაიკარგოს ან მოიპაროს. Macs-ს გააჩნია რეზერვის შექმნის საკუთარი პროგრამული უზრუნველყოფა Time Machine-ი, რომელიც გამოიყენება გარე საცავ მოწყობილობასთან ერთად; Windows-ის მოწყობილობებისათვის, File History-ი გთავაზობთ მსგავს ფუნქციონალს. iPhone-ებს და Android-ებს შეუძლია ავტომატურად შექმნას უმნიშვნელოვანესი კონტენტის ასლი ქლაუდზე, თუ ის ჩართულია თქვენი ტელეფონის პარამეტრებიდან. თუ თქვენი ორგანიზაცია იყენებს ქლაუდ-საცავს (როგორიცაა Google Drive-ი), Google-ის წაშლის ან თქვენი მონაცემების ავარიული განადგურების რისკი საკმაოდ დაბალია, თუმცა, ადამიანური შეცდომა (როგორიცაა მნიშვნელოვანი ფაილების შემთხვევით წაშლა) მაინც შესაძლებელია. შესაძლოა ღირებული იყოს Backupify-ის ან SpinOne Backup-ის მსგავსი ქლაუდ-რეზერვის გადაწყვეტების შესწავლა. თუ მონაცემები ინახება ადგილობრივ სერვერზე და/ან ადგილობრივ მოწყობილობებში, უსაფრთხო რეზერვი კიდევ უფრო მნიშვნელოვანი ხდება. შეგიძლიათ მოახდინოთ თქვენი ორგანიზაციის მონაცემების სარეზერვო ასლის შექმნა გარე მყარ დისკზე, თუმცა, აუცილებლად დაშიფრეთ ხსენებული მყარი დისკი ძლიერი პაროლით. Time Machine-ს შეუძლია დაშიფროს თქვენი მყარი დისკები ან თქვენ შეგიძლიათ გამოიყენოთ დაშიფვრის სანდო ინსტრუმენტები მთელი მყარი დისკისთვის, როგორიცაა VeraCrypt-ი ან BitLocker-ი. აუცილებლად შეინახეთ ნებისმიერი სარეზერვო მოწყობილობები სხვა მოწყობილობებისაგან და ფაილებისაგან განცალკევებულ ადგილზე. გახსოვდეთ, რომ ხანძარი ანადგურებს როგორც თქვენს კომპიუტერებს, ისე მათი სარეზერვო საშუალებებს, რომლებიც საერთოდ არ დაგირეზერვებიათ. დაფიქრდით ასლის მაქსიმალურად უსაფრთხო ადგილას შენახვაზე, როგორიცაა სეიფის სადეპოზიტო ყუთი.

შენიშვნა: თუ იყენებთ ქლაუდ-პროვაიდერს ქვეყანაში, სადაც მოქმედებს მონაცემთა ლოკალიზაციის სპეციალური კანონმდებლობა, მიიღეთ იურისტების კონსულტაცია, რათა უკეთ გესმოდეთ როგორ შეიძლება ქლაუდ-საცავის გამოყენება აკმაყოფილებდეს ნებისმიერ ადგილობრივ მოთხოვნას. მაგალითად, ქლაუდ-საცავის არაერთი პროვაიდერი, მათ შორის, Google-ი და Microsoft-ი, დღეისათვის გთავაზობთ ფუნქციებს, რომლებიც სთავაზობს ზოგიერთ მომხმარებელს აირჩიოს ქლაუდზე მისი მონაცემების გეოგრაფიული მდებარეობა.



ორგანიზაციული ქლაუდ-პროფილების უსაფრთხოების ამაღლება

თუ თქვენი ორგანიზაცია გადაწყვეტს გამართოს დომენი Google Workspace-ში ან Microsoft 365-ში, იცოდეთ, რომ ორივე კომპანია გთავაზობთ უსაფრთხოების (ხშირად, უფასოდ) უფრო მაღალ დონეებს სამოქალაქო საზოგადოებრივი ორგანიზაციებისათვის. Google-ის „გაუმჯობესებული დაცვის პროგრამა“ და Microsoft's AccountGuard-ი უფრო მტკიცე უსაფრთხოებას სთავაზობს თქვენი ორგანიზაციის ქლაუდ-პროფილებს და გეხმარებათ ფიშინგის და პროფილის გატეხის ალბათობის მნიშვნელოვნად შემცირებაში. თუ მიგაჩნიათ, რომ თქვენი ორგანიზაცია უფლებამოსილია და დაინტერესებულია თქვენი ორგანიზაციის ერთ-ერთ სქემაში ჩართვით, ეწვიეთ ზემოხსენებულ ვებგვერდებს ან დაუკავშირდით cyberhandbook@ndi.org შემდგომი დახმარებისათვის.



მონაცემების უსაფრთხოდ შენახვა

- **შეინახეთ სენსიტიური მონაცემები მხოლოდ სანდო ქლაუდ-საცავის სერვისში.**
  - უზრუნველყავით, რომ ნებისმიერ დაკავშირებულ პროფილს, რომელიც გამოიყენება აღნიშნულ სერვისზე წვდომისათვის, გააჩნდეს ძლიერი პაროლი და 2FA-ი.
- **შემოიღეთ და აღასრულეთ პოლიტიკა, რათა შეიზღუდოს გაზიარების პარამეტრები ქლაუდის ფარგლებში.**
  - აწარმოეთ მთელი პერსონალის ტრენინგი მასზედ, თუ როგორ უნდა მოხდეს დოკუმენტების მართებული გაზიარება (და არა ზედმეტად გაზიარება).
- **თუ თქვენი ორგანიზაცია გადაწყვეტს შეინახოს მონაცემები ადგილობრივად, გასწიეთ ხარჯი კვალიფიცური IT-ის პერსონალისათვის.**
- **უსაფრთხოდ შეინახეთ თქვენი მონაცემების რეზერვი - დაშიფრეთ სარეზერვო მყარი დისკები ან სხვა სარეზერვო მოწყობილობები.**



უსაფრთხოების დაცვა ინტერნეტში

უსაფრთხოების კულტურის დანერგვა

მყარი საფუძველი: პროფილების და მოწყობილობების დაცვა

უსაფრთხო კომუნიკაცია და მონაცემების შენახვა

უსაფრთხოების დაცვა ინტერნეტში

ფიზიკური უსაფრთხოების დაცვა

როგორ იქცევით, როცა საქმე ცუდადაა

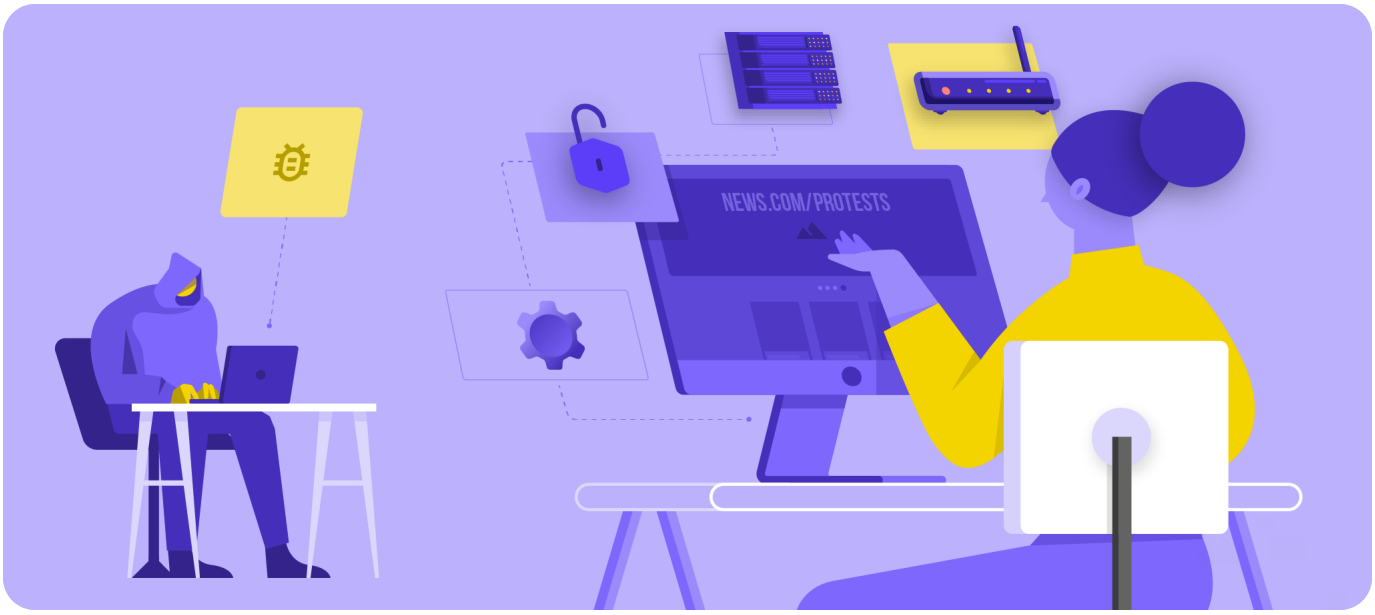
თქვენი ტელეფონით ან კომპიუტერით ინტერნეტით სარგებლობისას, თქვენს აქტივობას ბევრი რამის თქმა შეუძლია თქვენს და თქვენი ორგანიზაციის შესახებ.

მნიშვნელოვანია დატოვოთ სენსიტიური ინფორმაცია – როგორიცაა მომხმარებლის სახელები და პაროლები, რომლებსაც ჩაწერთ ვებსაიტზე, თქვენი პოსტები სოციალურ მედიაში ან კონკრეტულ კონტექსტებში იმ ვებგვერდების დასახელებების ჩათვლით, რომლებსაც ეწვევით – ცნობისმოყვარე თვალის ხედვის არეალს მიღმა. კონკრეტულ გვერდებზე თუ აპებზე თქვენი წვდომის ბლოკირება ან შეზღუდვა ასევე საყოველთაო შეშფოთების საგანია. ხსენებული ორი პრობლემა – ინტერნეტში თვალთვალი და ინტერნეტ-ცენზურა – მჭიდრო კავშირშია, ხოლო მათი გავლენის შემცირების სტრატეგიები მსგავსია.

უსაფრთხო ბრაუზინგი

HTTPS-ის გამოყენება

თქვენი მეტოქის მიერ თქვენი ორგანიზაციის ონლაინ კონტროლის უნარის შეზღუდვისკენ მიმართული უმნიშვნელოვანესი ნაბიჯია იმ ინფორმაციის მინიმიზაცია, რომელიც ხელმისაწვდომია თქვენი და თქვენი კოლეგების ინტერნეტ-აქტივობების შესახებ. მუდამ დარწმუნდით, რომ უკავშირდებით ვებგვერდებს უსაფრთხოდ: დარწმუნდით, რომ URL-ი (ლოკაცია) იწყება „https“-ით და უჩვენებს პატარა ბოქლომს თქვენი ბრაუზერის მისამართის ზოლში. ინტერნეტში **დაშიფვრის გარეშე** ბრაუზინგისას დაუცველია თქვენს მიერ ვებგვერდზე მითითებული ინფორმაცია (მაგალითად, პაროლები, ანგარიშის ნომრები ან შეტყობინებები) იმ ვებგვერდების და გვერდების რეკვიზიტები, რომლებსაც ეწვევით. აღნიშნული ნიშნავს, რომ (1) ნებისმიერ ჰაკერს თქვენს ქსელში, (2) თქვენი ქსელის ადმინისტრატორს, (3) თქვენს ISP-ს და ნებისმიერ ორგანოს, რომელსაც შესაძლოა გაუზიაროს მან მონაცემები (მაგალითად, სამთავრობო უწყებები), (4) იმ გვერდის ISP-ი, რომელსაც თქვენს ეწვევით და ნებისმიერი ორგანიზაცია, რომელსაც შესაძლოა გაუზიაროს *მან* მონაცემები და, რა თქმა უნდა, (5) თვით ვებგვერდი, რომელსაც ეწვევით, ყველა მათგანს გააჩნია წვდომა საკმაოდ ვრცელ, პოტენციურად სენსიტიურ ინფორმაციაზე.



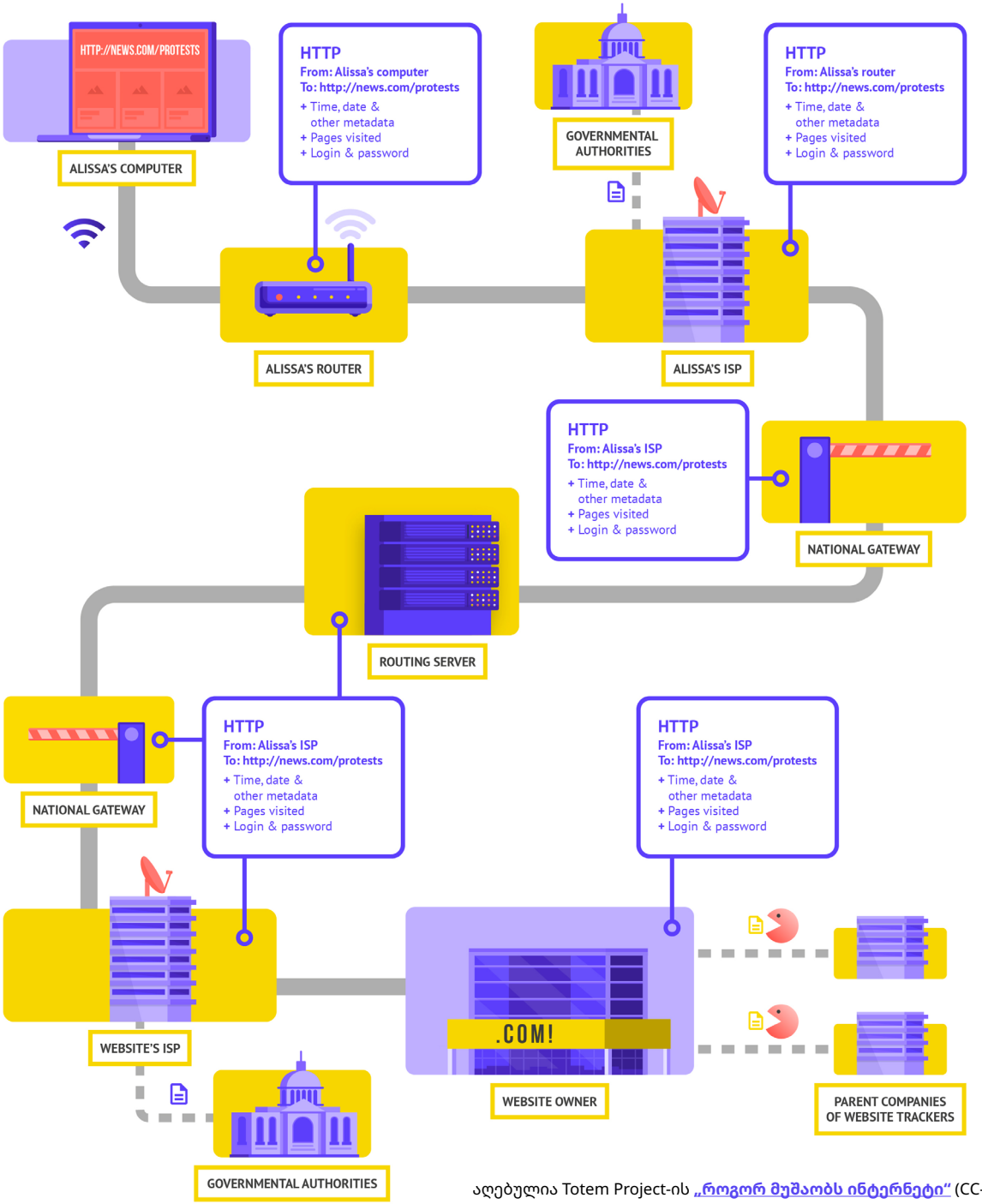
თვალთვალი, ცენზურა და სამოქალაქო საზოგადოება

მთავრობები სულ უფრო ხშირად იყენებენ საკუთარ გავლენას და უფლებამოსილებას ინტერნეტ-სერვისის პროვაიდერებთან და სხვა ადგილობრივ ინტერნეტ-ინფრასტრუქტურასთან მიმართებაში, რათა ხელი შეუშალონ ცალკეულ პიროვნებებს და სამოქალაქო საზოგადოების ჯგუფებს ინტერნეტით ინფორმაციაზე წვდომაში. ზოგიერთ შემთხვევაში, ინტერნეტის ხსენებული წყვეტა მიზნად ისახავს საკვანძო კომუნიკაციის და ინფორმაციის გაზიარების პლატფორმების, მათ შორის, სოციალური მედიის და ახალი ამბების გვერდების შეფერხებას. მაგალითად, სამხედრო გადატრიალებით გამოწვეული პროტესტის პასუხად მიანმას სამხედრო უწყებამ უბრძანა მობილურ ოპერატორებს დროებით გამოერთო მობილური მონაცემების მთელი ქსელი ქვეყანაში. ეს მოხდა Facebook-ში, Twitter-ში და Instagram-ში უფრო მეტად მიზნობრივი ბლოკირებიდან მოკლე ხანში. გარდა ინტერნეტზე წვდომის და ვებგვერდების ბლოკირებისა, მთავრობები და სხვა ბოროტი ძალები მთელს მსოფლიოში იყენებენ სულ უფრო მეტად წვდომად სათვალთვალო ტექნოლოგიას მოქალაქეების ონლაინ საქმიანობის მონიტორინგისათვის. მაგალითად, Freedom House-ის „თავისუფლება ქსელში 2020“ ანგარიშის თანახმად, უგანდის მთავრობამ პარტნიორული ურთიერთობა დაამყარა ჩინურ ტექ-კომპანია Huawei-თან, რათა **გაეკონტროლებინა ოპოზიციის რეიტინგი და მისი სამოქალაქო საქმიანობა** ქვეყანაში სადაო საპრეზიდენტო არჩევნების მომდევნო დღეს და შედეგების გამოცხადების შემდეგ.

ინფორმაციასთან წვდომაზე და მის ონლაინ თავისუფლებაზე ხსენებული შეტევების მზარდი სიხშირე ხაზს უსვამს, რამდენად მნიშვნელოვანია სამოქალაქო საზოგადოების ჯგუფებისათვის ესმოდეთ ინტერნეტში მუშაობის რისკი და შეიმუშაონ გეგმები მასზედ, თუ როგორ მოახდინონ დაკავშირება, როცა კავშირი შეფერხებულია.



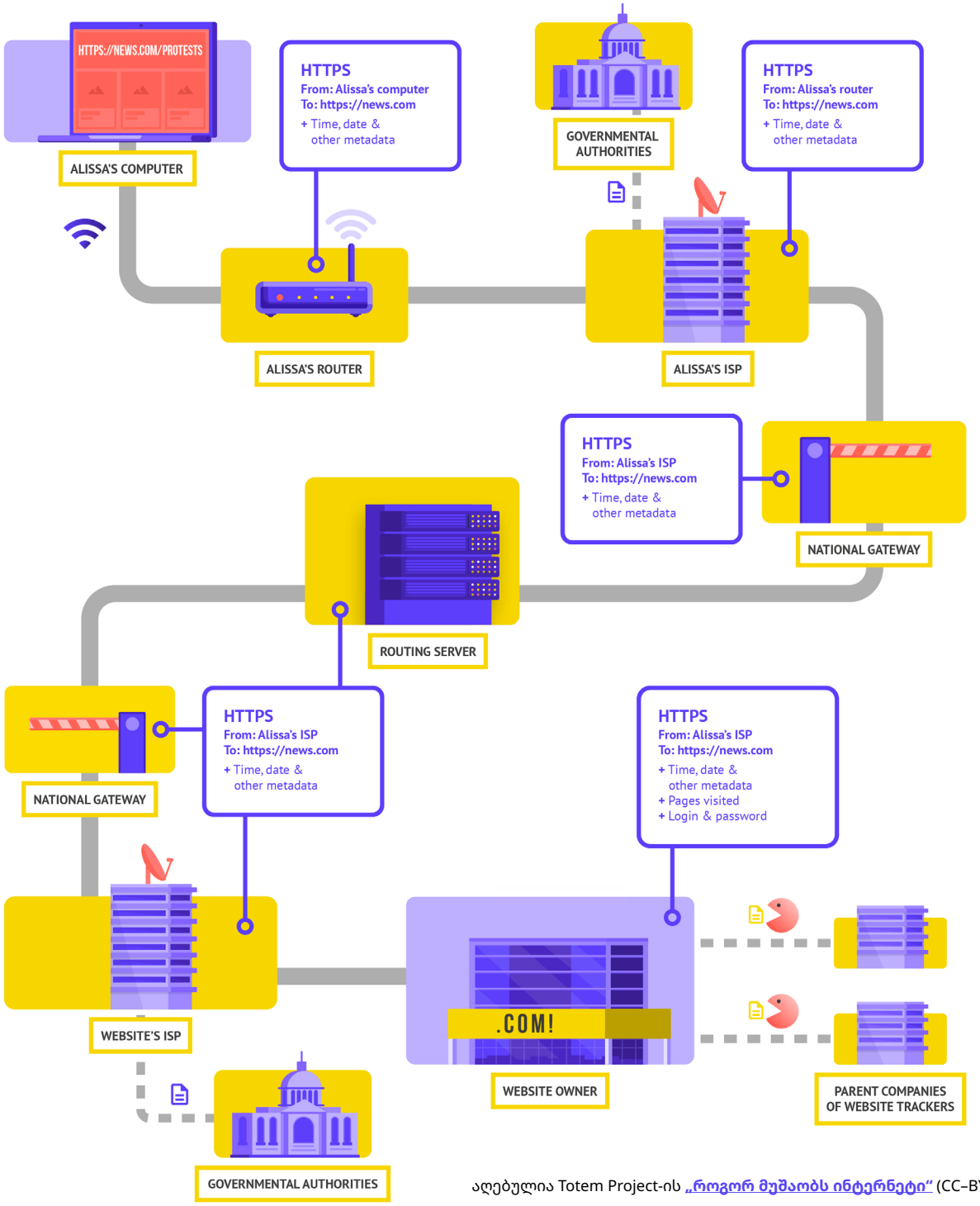
მოდით ავიღოთ მაგალითი რეალური ცხოვრებიდან მასზედ, თუ როგორ გამოიყურება ბრაუზინგი დაშიფვრის გარეშე:



აღებულია Totem Project-ის „როგორ მუშაობს ინტერნეტი“ (CC–BY–NC–SA)

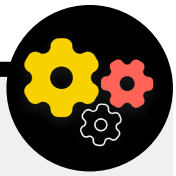
დაშიფვრის გარეშე ბრაუზინგისას დაუცველია ყველა თქვენი მონაცემი. როგორც ზემოთ ხედავთ, მეტოქეს შეუძლია, ნახოს, სად ხართ, რომ ეწვიეთ news.com-ს, ყურადღებით ათვალიერებთ გვერდს თქვენს ქვეყანაში პროტესტის შესახებ და ხედავს თქვენს პაროლს, რომელსაც აზიარებთ თავად ვებგვერდის სისტემაში შესასვლელად. ასეთი ინფორმაცია უცხო ხელში მოხვედრისას არა მხოლოდ დაუცველს ხდის თქვენს პროფილს, არამედ, ასევე, აძლევს პოტენციურ მეტოქეს ზუსტ წარმოდგენას, რას შეიძლება აკეთებდეთ ან რაზე შეიძლება ფიქრობდეთ.

HTTPS-ის („s"-ი აღნიშნავს დაცულს) გამოყენება გულისხმობს, რომ დაშიფვრა მუშაობს. აღნიშნული გთავაზობთ გაცილებით მეტ დაცვას. მოდით ვნახოთ როგორ გამოიყურება ბრაუზინგი HTTPS-ით (იგივე დაშიფვრა) :



აღებულია Totem Project-ის „როგორ მუშაობს ინტერნეტი" (CC–BY–NC–SA)

HTTPS-ის მუშაობისას, პოტენციურ მეტოქეს აღარ შეუძლია თქვენი პაროლის თუ იმ სხვა სენსიტიური ინფორმაციის დანახვა, რომელიც შესაძლოა გააზიაროთ ვებგვერდზე. თუმცა, მათ მაინც შეუძლიათ ნახონ რომელ დომენს (მაგალითად, news.com-ი) ეწვევით. და მიუხედავად იმისა, რომ HTTPS-ი ასევე დაშიფრავს ინფორმაციას ვებგვერდის ფარგლებში კონკრეტული გვერდების შესახებ (მაგალითად, website.com/protests-ი), რომელსაც ეწვევით, მახვილგონიერ მეტოქეს მაინც შეუძლია ხსენებული ინფორმაციის დანახვა თქვენი ინტერნეტ-ტრაფიკის გადახედვის გზით. HTTPS-ის მუშაობისას, მეტოქემ შესაძლოა იცოდეს, რომ თქვენ ეწვევით news.com-ს, თუმცა, მას არ შეეძლება ნახოს თქვენი პაროლი და მისთვის უფრო რთული იქნება (თუმცა, არა შეუძლებელი) ნახოს, რომ ათვალიერებთ ინფორმაციას პროტესტის შესახებ (ამ კონკრეტულ მაგალითში). ეს მნიშვნელოვანი განსხვავებაა. ვებგვერდზე გადასვლამდე ან სენსიტიური ინფორმაციის ჩაწერამდე მუდამ შეამოწმეთ, რომ HTTPS-ი მუშაობს. ასევე შეგიძლია გამოიყენოთ **HTTPS Everywhere-ის ბრაუზერის გაფართოება**, რათა უზრუნველყოთ, რომ მუდამ იყენებთ HTTPS-ს ან, თუ იყენებთ Firefox-ს, ჩართეთ **HTTPS ერთადერთი რეჟიმი** ბრაუზერში. თუ მიიღეთ გაფრთხილება თქვენი ბრაუზერიდან, რომ ვებგვერდი შესაძლოა არ იყოს უსაფრთხო, ნუ უგულებელყოფთ მას. რაღაც არაა სწორად. ეს შესაძლოა იყოს მსუბუქი – მაგალითად ვებგვერდის უსაფრთხოების სერტიფიკატის ვადის გასვლა – ან ვებგვერდი შესაძლოა იყოს ბოროტი განზრახვით გატეხილი ან გაყალბებული. როგორც არ უნდა იყოს, მნიშვნელოვანია ყურადღება მივაქციოთ გაფრთხილებას და აღარ შევიდეთ ვებგვერდზე. HTTPS-ი უმნიშვნელოვანესია და დაშიფრული DNS-ი უზრუნველყოფს გარკვეულ დამატებით დაცვას თვალთვალის და ვებგვერდის ბლოკირებისაგან, თუმცა, თუ თქვენი ორგანიზაცია შეშფოთებულია თქვენს ონლაინ საქმიანობაზე მიზანმიმართული თვალთვალის გამო და განიცდის მკაცრ ონლაინ ცენზურას (როგორიცაა ვებგვერდების და აპების ბლოკირება), შესაძლოა, გსურდეთ სანდო ვირტუალური კონფიდენციალური ქსელის (VPN-ი) გამოყენება.



დაშიფრული DNS-ის გამოყენება

თუ გსურთ გაურთულოთ (თუმცა, არა შეუძლებელი გახადოთ) ISP-თვის იმ ვებგვერდის დეტალების შეტყობა, რომელსაც ეწვიეთ, შეგიძლიათ გამოიყენოთ დაშიფრული DNS-ი.

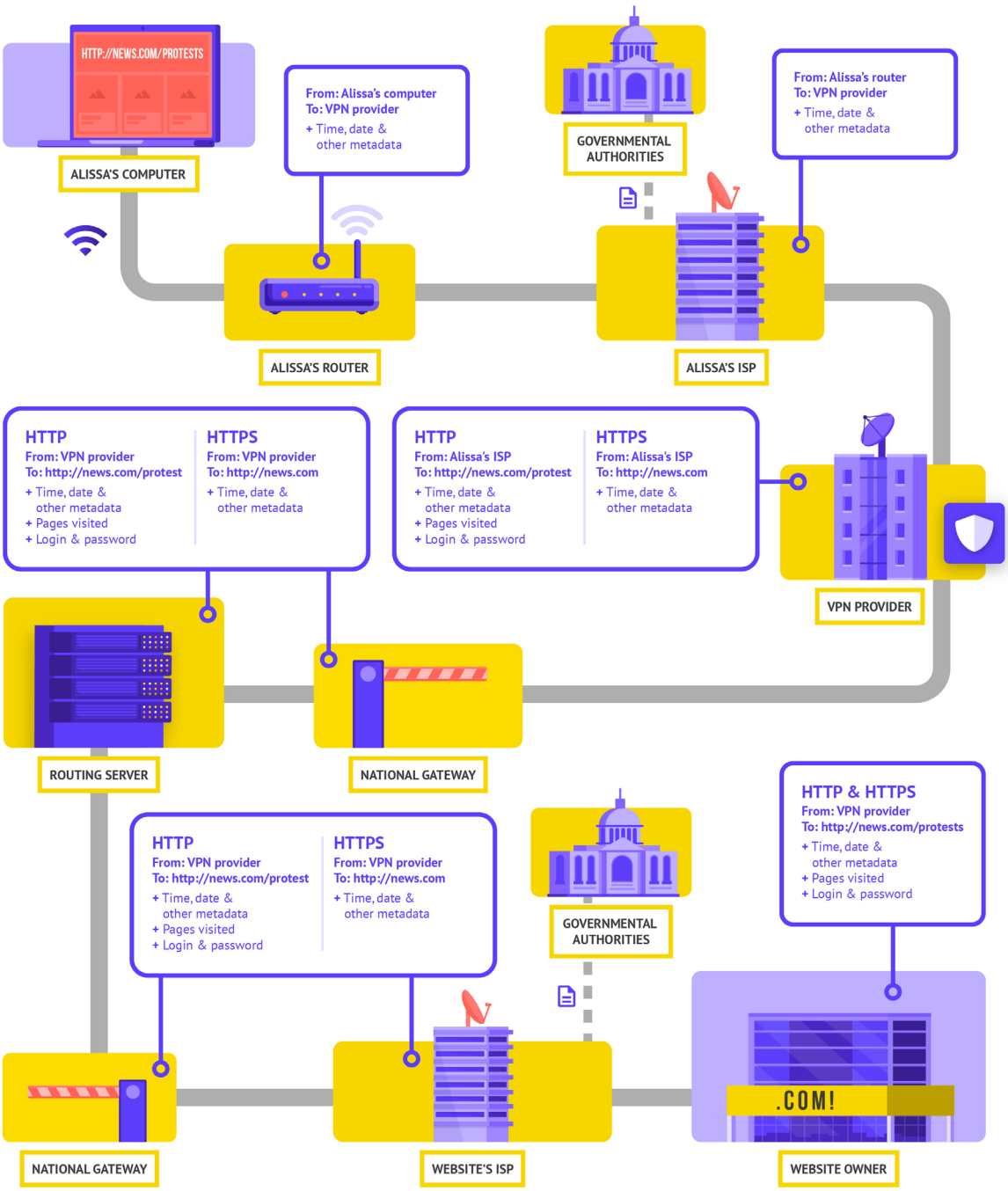
თუ **გაინტერესებთ**, DNS-ი ნიშნავს დომენის დასახელების სისტემას. რეალურად, ესაა ინტერნეტის ტელეფონის ნომრების წიგნაკი, რომელიც გარდაქმნის ადამიანისათვის მოსახერხებელ დომენის დასახელებებს (მაგალითად, ndi.org) ქსელისათვის მოსახერხებელ ინტერნეტ-პროტოკოლის (IP-ი) მისამართებად. ეს საშუალებას აძლევს ადამიანებს გამოიყენონ ბრაუზერები ინტერნეტ-რესურსების მარტივად მოძიების და ვებგვერდებზე მოხვედრის მიზნით. თუმცა, უპირობოდ, DNS-ი არაა დაშიფრული.

დაშიფრული DNS-ის გამოყენების და, ამავე დროს, თქვენი ინტერნეტ-ტრაფიკის დაცვის გაძლიერების მიზნით ერთი მარტივი ოფციაა ჩამოტვირთოთ და ჩართოთ **აპი Cloudflare's 1.1.1.1** თქვენს კომპიუტერში ან მობილურ მოწყობილობაში. დაშიფრული DNS-ის სხვა ოფციები, მათ შორის, Google-ის 8.8.8.8, ხელმისაწვდომია, თუმცა საჭიროებს **მეტ ტექნიკურ ნაბიჯებს** კონფიგურაციის მიზნით. თუ იყენებთ ბრაუზერს Firefox-ი, დაშიფრული DNS-ი ჩართულია უპირობოდ. Chrome-ის ან Edge-ის მომხმარებელს შეუძლია, **აამუშაოს დაშიფრული DNS-ი** ბრაუზერის უსაფრთხოების ამაღლების პარამეტრებში „use secure DNS" ჩართვით და აირჩევს რა „With: Cloudflare (1.1.1.1)"-ს ან პროვაიდერს საკუთარი სურვილისამებრ.

Cloudflare's 1.1.1.1-ი WARP-ით დაშიფრავს თქვენს DNS-ს და დაშიფრავს თქვენი ბრაუზინგის მონაცემებს - გასწევს ტრადიციული VPN-ის მსგავს სერვისს. მიუხედავად იმისა, რომ WARP-ი არ იცავს სრულად თქვენს ლოკაციას ყველა იმ ვებგვერდისაგან, რომელსაც ეწვევით, ის მარტივად გამოსაყენებელი ფუნქციაა, რომელსაც შეუძლია დაეხმაროს თქვენი ორგანიზაციის პერსონალს ისარგებლოს დაშიფრული DNS-ით და მიიღოს მეტი დაცვა თქვენი ISP-გან იმ სიტუაციაში, როცა სრული VPN-ი ან არ მუშაობს ან საჭიროებს საფრთხის კონტექსტის განსაზღვრას. WARP-ით აღჭურვილი 1.1.1.1-ის გაუმჯობესებულ DNS-ის პარამეტრებში, პერსონალს ასევე შეუძლია ჩართოს 1.1.1.1-ი ოჯახებისათვის, რათა უზრუნველყოს დამატებითი დაცვა ინტერნეტში მუშაობისას საზიანო პროგრამისგან დასაცავად.

რა არის VPN-ი?

VPN-ი რეალურად წარმოადგენს გვირაბს, რომელიც იცავს თქვენს ინტერნეტ-ტრაფიკს თქვენს ქსელში მოქმედი ჰაკერების, თქვენი ქსელის ადმინისტრატორის და იმ ნებისმიერი პირის მიერ თვალთვალის და ბლოკირებისაგან, რომელსაც შესაძლოა გაუზიარონ მონაცემები ხსენებულებმა. თუმცა, მაინც მნიშვნელოვანია HTTPS-ის გამოყენება და იმის უზრუნველყოფა, რომ თქვენ ენდობით თქვენი ორგანიზაციის მიერ გამოყენებულ VPN-ს. აი მაგალითი იმისა, თუ როგორ გამოიყურება VPN-ით ბრაუზინგი:



აღებულია Totem Project-ის „როგორ მუშაობს ინტერნეტი“ (CC–BY–NC–SA)

VPN-ების უკეთ აღწერის მიზნით, მოცემულ სექციაში მოცემულია მითითება EFF-ის „თვალთვალისაგან თავდაცვის სახელმძღვანელოზე“:

ტრადიციული VPN-ები მიზანია შენიღბონ თქვენი რეალური ქსელური IP-ის მისამართი და შექმნან დაშიფრული გვირაბი ინტერნეტ-ტრაფიკისათვის თქვენს კომპიუტერს (ან ტელეფონს თუ ქსელში ჩართულ ნებისმიერ „სმარტ“ მოწყობილობას) და VPN-ის სერვერს შორის. რადგან ტრაფიკი გვირაბში დაშიფრულია და ეგზავნება თქვენს VPN-ს, ISP-ების ან საჯარო Wi-Fi-ში ჩართული ჰაკერების მსგავსი მესამე მხარეებისათვის გაცილებით რთულია განახორციელონ თქვენი ტრაფიკის მონიტორინგი, მოდიფიცირება ან ბლოკირება. თქვენგან VPN-ის მიმართულებით გვირაბის გავლის შემდეგ თქვენი ტრაფიკი გადის VPN-დან მისი საბოლოო დანიშნულების მიმართულებით და ნიღბავს თქვენს საწყის IP-ის მისამართს. აღნიშნული გეხმარებათ შენიღბოთ თქვენი ფიზიკური ლოკაცია ყველასათვის, ვინც თვალს ადევნებს ტრაფიკს მის მიერ VPN-დან გასვლის შემდეგ. ხსენებული გთავაზობთ მეტ კონფიდენციალურობას და უსაფრთხოებას, მაგრამ, VPN-ის გამოყენება არ განიჭებს სრულ ონლაინ ანონიმურობას: თქვენი ტრაფიკი მაინც ხილვადია VPN-ის ოპერატორისათვის. თქვენი ISP-თვის ასევე ცნობილი იქნება, რომ იყენებთ VPN-ს, რამაც შესაძლოა აამაღლოს თქვენს მიერ განცდილი რისკი.

ეს ნიშნავს, რომ **მნიშვნელოვანია VPN-ის სანდო პროვაიდერის შერჩევა.** ზოგ ადგილებში, მაგალითად ირანში, მტრულ მთავრობებს გამართული აქვთ საკუთარი VPN-ები, რათა შეეძლოთ თვალი მიადევნონ მოქალაქეების ქმედებებს. იმ VPN-ის მოსაძიებლად, რომელიც მისაღებია თქვენი ორგანიზაციის და მისი პერსონალისათვის, შეგიძლიათ შეაფასოთ VPN-ები გამომდინარე მათი ბიზნეს-მოდელებიდან და რეპუტაციიდან, მათ მიერ შეგროვებადი თუ შეუგროვებადი მონაცემებიდან და, რა თქმა უნდა, თვით ინსტრუმენტის უსაფრთხოებიდან.

რატომ არ უნდა გამოიყენოთ უბრალოდ უფასო VPN-ი? მოკლე პასუხი ისაა, რომ უფასო VPN-ების უმეტესობა, მათ შორის, ისინი, რომლებიც წინასწარაა ინსტალირებული ზოგიერთ სმარტფონში, შეიცავს ხაფანგს. ყველა ბიზნეს- და სერვის-პროვაიდერის მსგავსად, VPN-ემა თავად უნდა შეინახოს თავი. თუ VPN-ი არ ყიდის საკუთარ სერვისს, როგორ ახერხებს ის ბიზნესში დარჩენას? ითხოვს ის შემოწირულობებს? აქვს გადასახადი პრემიუმ-სერვისისათვის? უჭერს მას მხარს საქველმოქმედო ორგანიზაციები ან ფონდები? სამწუხაროდ, არაერთი უფასო VPN-ი ფულს შოულობს თქვენი მონაცემების შეგროვებით და გაყიდვით.

VPN-ის პროვაიდერი, რომელიც, უპირველეს ყოვლისა, არ აგროვებს მონაცემებს არის საუკეთესო არჩევანი. თუ მონაცემები არ გროვდება, ისინი ვერ გაიყიდება ან გადაეცემა მთავრობას მოთხოვნის შემთხვევაში. VPN-ის პროვაიდერის კონფიდენციალურობის პოლიტიკის გაცნობისას ნახეთ აგროვებს თუ არა VPN-ი რეალურად მომხმარებლის მონაცემებს. თუ ის ნათლად არ აცხადებს, რომ მომხმარებლის დაკავშირების მონაცემები არ აღირიცხება, არის შანსი, რომ ისინი აღირიცხება. იმ შემთხვევაშიც კი, როცა კომპანია ამტკიცებს, რომ არ აღრიცხავს დაკავშირების მონაცემებს, ეს შესაძლოა, მაინც არ იყოს კეთილსინდისიერი ქცევის გარანტია.

მნიშვნელოვანია VPN-ის უკან მყოფი კომპანიის კვლევის წარმოება. მოწონებულია ის უსაფრთხოების დამოუკიდებელი ექსპერტების მიერ? არსებობს ახალი ამბების სამსახურების მიერ VPN-ის თაობაზე დაწერილი სტატიები? ამხილეს ის ოდესმე მომხმარებლის შეცდომაში შეყვანაში ან ტყუილში? თუ VPN-ი დაფუძნებულია ინფორმაციის უსაფრთხოების საზოგადოებისათვის ცნობილი ადამიანების მიერ, ის, სავარაუდოდ, უფრო სანდოა. სკეპტიკურად მიუდექით VPN-ს, რომელიც გთავაზობთ სერვისს, რომლის გამოც არავინ რისკავს საკუთარი რეპუტაციით ან რომელიც ეკუთვნის კომპანიას, რომელსაც არავინ იცნობს.

ყალბი VPN-ები რეალურ სამყაროში

2017 წ. ბოლოს, ქვეყანაში საპროტესტო ტალღის მატების შემდეგ, ირანელები აღმოაჩინეს პოპულარული VPN-ის „უფასო“ (მაგრამ ყალბი) ვერსია, რომელზე ინფორმაციაც გაზიარდებოდა ტექსტური შეტყობინებების საშუალებით. უფასი VPN-ი, რომელიც რეალურად არ მუშაობდა, იძლეოდა იმ დროისთვის ადგილობრივად ბლოკირებულ Telegram-ზე წვდომის დაპირებას. სამწუხაროდ, ყალბი აპლიკაცია სხვა არაფერი იყო, თუ არა საზიანო პროგრამა, რომელიც საშუალებას აძლევდა ორგანოებს თვალი ედევნებინათ მისი ჩამომტვირთავების გადაადგილების და კომუნიკაციისათვის.

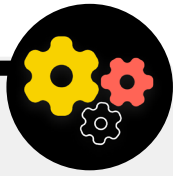


ამგვარად, რომელი VPN-ი უნდა გამოვიყენოთ?

თუ თქვენი ორგანიზაციისთვის მნიშვნელოვანია VPN-ის გამოყენება, ამისთვის რამდენიმე სანდო ვარიანტია, მათ შორის, TunnelBear და ProtonVPN. კიდევ ერთი ოფციაა თქვენი საკუთარი სერვერის კონფიგურაცია Jigsaw-ის Outline-ის გამოყენებით, სადაც თქვენს პროფილს მართავს არა კომპანია, არამედ თქვენ თავად თავად უნდა გამართოთ თქვენი საკუთარი სერვერი. თუ თქვენი კომპანია ცოტა უფრო დიდია, შესაძლოა გსურდეთ ბიზნეს-VPN-ი, რომელიც გთავაზობთ პროფილის მართვის ფუნქციებს, როგორიცაა TunnelBear-ის Teams-ის სქემა. სამოქალაქო საზოგადოების და ადამიანის უფლებების დაცვის სექტორში მომუშავე ზოგიერთი შესაფერისი ორგანიზაციისათვის, TunnelBear-ი უზრუნველყოფს შეღავათებს საკუთარი VPN-ის უფასო გამოყენებისათვის (რომელიც, ჩვეულებრივ, თვეში დაახლოებით 3 აშშ დოლ. ღირს). თუ მიგაჩნიათ, რომ თქვენი ორგანიზაცია შესაფერისია და ხართ დაინტერესებული, ინფორმაციისთვის დაგვიკავშირდით შემდეგ მისამართზე:

cyberhandbook@ndi.org - ს.
მიუხედავად იმისა, რომ თანამედროვე VPN-ების უმეტესობა გაუმჯობესდა მუშაობის და სიჩქარის თვალსაზრისით, აჯობებს გახსოვდეთ, რომ VPN-ის გამოყენებამ შესაძლოა შეანელოს თქვენი ბრაუზინგის სიჩქარე, თუ ხართ მეტად დაბალი წარმადობის ქსელში, განიცდით ხანგრძლივ დაყოვნებას თუ ქსელის შეფერხებებს ან ინტერნეტის წყვეტად მოწოდებას. თუ თქვენი ქსელი უფრო სწრაფია, შეგიძლიათ, ყოველთვის ნაგულისხმევად გამოიყენოთ VPN.

თუ უწევთ რეკომენდაციას, რომ პერსონალმა გამოიყენოს VPN-ი, ასევე მნიშვნელოვანია, უზრუნველყოთ, რომ ხალხს VPN-ი ჩართული ჰქონდეს. შესაძლოა ისედაც ნათელი იყოს, მაგრამ VPN-ი, რომელიც ინსტალირებულია, მაგრამ არ მუშაობს ვერ უზრუნველყოფს რაიმე დაცვას.



ანონიმურობა Tor-ის საშუალებით

გარდა VPN-ებისა, შესაძლოა გაგიგონიათ Tor-ის, როგორც ინტერნეტის გამოყენებისას მეტი უსაფრთხოების ინსტრუმენტის შესახებ. მნიშვნელოვანია გვესმოდეს რა არის ორივე, რატომ შესაძლოა იყენებდეთ ერთს ან მეორეს და როგორ შესაძლოა იმოქმედოს თქვენს ორგანიზაციაზე ორივემ.

Tor-ს წარმოადგენს ინტერნეტში მონაცემთა ანონიმურად გადაცემის პროტოკოლს რომელიც მიმართავს შეტყობინებებს ან მონაცემებს დეცენტრალიზებული ქსელის გავლით. Tor-ის მუშაობის შესახებ შეგიძლიათ გაიგოთ აქ, თუმცა, მოკლედ რომ ვთქვათ, ის მიმართავს თქვენს ტრაფიკს საბოლოო დანიშნულების გზაზე მრავალი პუნქტის გავლით ისე, რომ არცერთ ცალკეულ პუნქტს გააჩნია საკმარისი ინფორმაცია თქვენი ვინაობის და ონლაინ თქვენი საქმიანობის მყისიერად გასარკვევად.

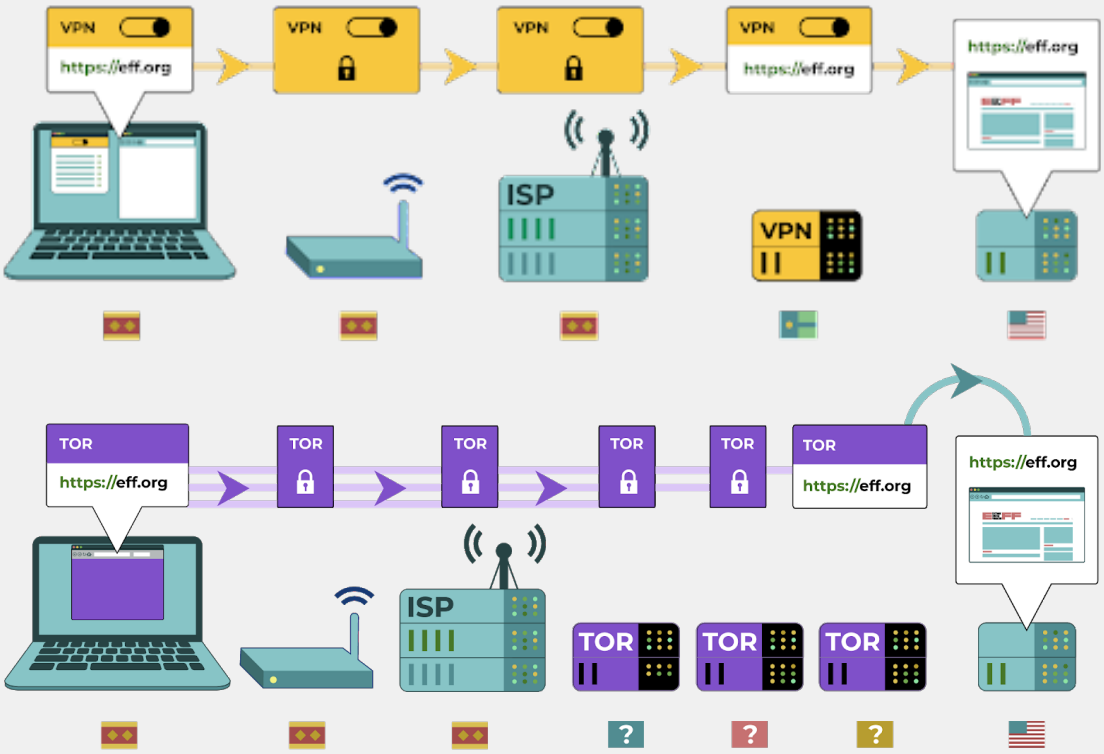
Tor-ი განსხვავდება VPN-გან რამდენიმე ფაქტორით. ყველაზე ფუნდამენტურია, რომ ის განსხვავდება იმით, რომ არ ეფუძნება რომელიმე კონკრეტული პუნქტის ნდობას (როგორც VPN-ის პროვაიდერი).

EFF-ის მიერ შედგენილი ეს გრაფიკი უჩვენებს განსხვავებას ტრადიციულ VPN-ს და Tor-ს შორის.

Tor-ის გამოყენების უმარტივესი გზაა Tor-ის ვებ-ბრაუზერი.

ის მუშაობს, როგორც ნებისმიერი ნორმალური ბრაუზერი, გარდა იმისა, რომ ის მიმართავს ტრაფიკს Tor-ის ქსელში. შეგიძლიათ ჩამოტვირთოთ Tor-ის ბრაუზერი Windows-ის, Mac-ის, Linux-ის ან Android-ის მოწყობილობებისათვის. გახსოვდეთ, რომ Tor-ის ბრაუზერის გამოყენებისას იცავთ მხოლოდ ინფორმაციას, რომელზეც გაქვთ წვდომა **ბრაუზერში მუშაობისას.** ის არ უზრუნველყოფს რაიმე დაცვას სხვა აპის ან ჩამოტვირთული ფაილებისათვის, რომლებიც შესაძლოა გახსნათ ცალკე თქვენს მოწყობილობაში. ასევე გახსოვდეთ, რომ Tor-ი არ შიფრავს თქვენს ტრაფიკს, ამიტომ - VPN-ის გამოყენების მსგავსად - ჯერაც მნიშვნელოვანია ბრაუზინგისას გამოიყენოთ აღიარებული მეთოდიკა, როგორიცაა HTTPS-ი.

თუ გსურთ გააფართოვოთ Tor-ის ანონიმურობის დაცვის საშუალებები მთლიანად თქვენს კომპიუტერთან მიმართებაში, ტექნიკასთან მეგობრულ მომხმარებელს შეუძლია დააინსტალიროს Tor-ი, როგორც სისტემური ინტერნეტ-კავშირი ან გამოიყენოს Tails-ის ოპერაციული სისტემა, რომელიც უპირობოდ მიმართავს მთელს ტრაფიკს Tor-ის გავლით. Android-ის მომხმარებელს ასევე შეუძლია გამოიყენოს აპი Orbot-ი, რათა ამუშაოს Tor-ი მისი მოწყობილობის მთელი ინტერნეტ-ტრაფიკის და ყველა აპისათვის. მიუხედავად იმისა, თუ როგორ იყენებთ Tor-ს, მნიშვნელოვანია იცოდეთ, რომ მისი გამოყენებისას თქვენი ინტერნეტ პროვაიდერი ვერ ხედავს რომელ ვებგვერდებს



ეწვევით, თუმცა, „შეუძლია“ დაინახოს, რომ, როგორც ასეთი, იყენებთ Tor-ს. VPN-ის გამოყენების მსგავსად, ამან შესაძლოა მნიშვნელოვნად აამაღლოს თქვენი ორგანიზაციის რისკი, რადგან Tor-ი არაა მეტად ფართოდ გავრცელებული ინსტრუმენტი და, ამდენად, გამოირჩევა მეტოქეებისათვის, რომლებიც შესაძლოა აწარმოებდნენ თქვენი ინტერნეტ-ტრაფიკის მონიტორინგს.

ამგვარად, უნდა გამოიყენოს თქვენმა ორგანიზაციამ Tor-ი? პასუხი: გააჩნია. რისკის ქვეშ მყოფი ორგანიზაციების უმეტესობისთვის, სანდო VPN-ი, რომელსაც ყოველთვის სწორად გამოიყენებს მთელი პერსონალი, უნდა იყოს უმარტივესი, მაქსიმალურად მოსახერხებელი და, VPN-ის გლობალურად ფართო გამოყენების საუკუნეში, ნაკლებად უნდა იქონიოს საგანგაშო სიგნალები. თუმცა, თუ სანდო VPN-ი ძვირია თქვენთვის ან მუშაობთ გარემოში, სადაც VPN-ები, ჩვეულებრივ, იბლოკება, Tor-ი შესაძლოა კარგი ოფცია იყოს, კანონიერების შემთხვევაში, თვალთვალის გავლენის შეზღუდვის და ონლაინ ცენზურის თავიდან აცილების მიზნით.

არსებობს რაიმე მიზეზი, რის გამოც არ უნდა გამოვიყენოთ VPN-ი ან Tor-ი?

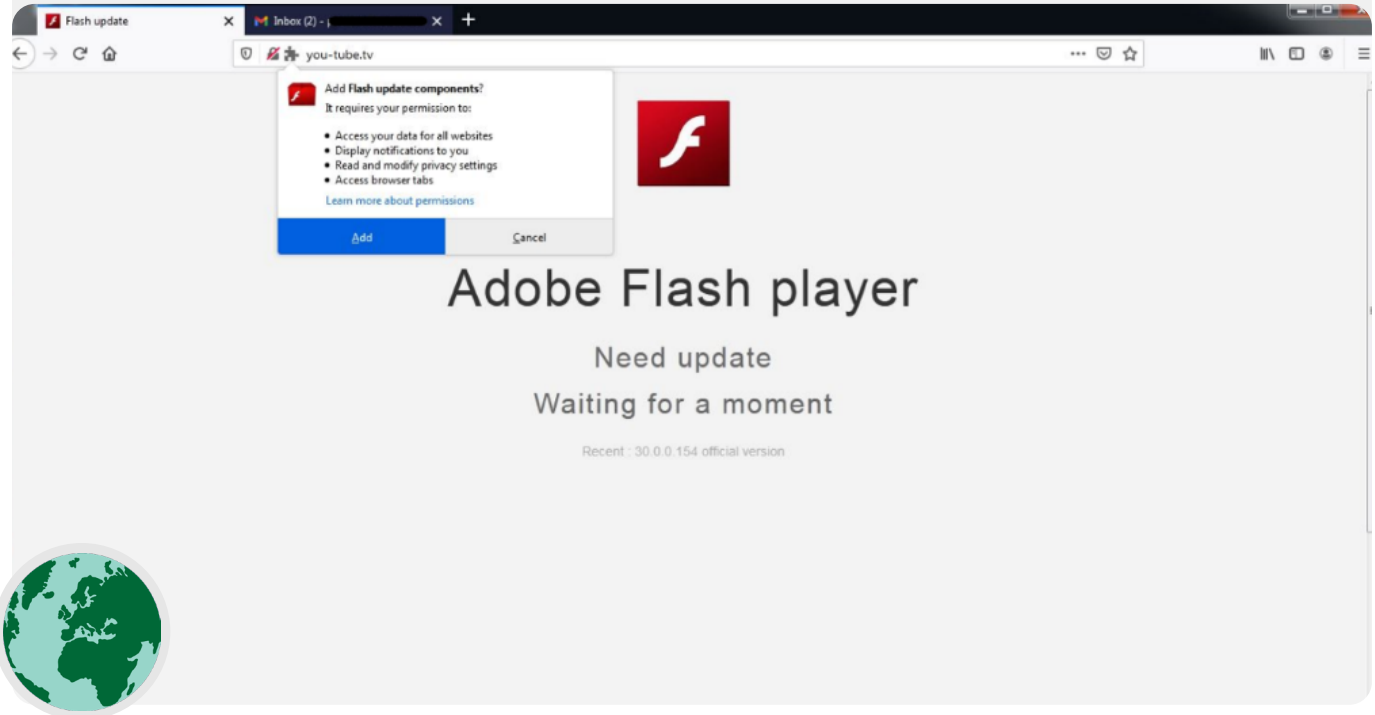
გარდა რეპუტაციის არმქონე VPN-ის სერვისის შესახებ შფოთვისა, გასათვალისწინებლად უდიდესი მნიშვნელობა აქვს მიიპყრობს თუ არა VPN-ის ან Tor-ის გამოყენება არასასურველ ყურადღებას ან, ზოგიერთი კანონმდებლობის ფარგლებში, ეწინააღმდეგება თუ არა ის კანონს. მიუხედავად იმისა, რომ თქვენს ISP-ს არ ეცოდინება რომელ ვებგვერდებს ეწვიეთ აღნიშნული სერვისების გამოყენებისას, მათ შეუძლიათ დაინახონ, რომ ჩართული გაქვთ Tor-ი ან VPN-ი. თუ ეს უკანონოა იქ, სადაც მუშაობს თქვენი ორგანიზაცია ან შესაძლოა მიიპყროს მეტი ყურადღება ან წარმოშვას მეტი რისკი, ვიდრე უბრალოდ ქსელში ჩართვამ სტანდარტული HTTPS-ით და დაშიფრული DNS-ით, ალბათ VPN-ი ან, განსაკუთრებით, Tor-ი (რომელიც გაცილებით ნაკლებად გამოიყენება და, ამდენად, უფრო მეტად „საგანგაშოა“) არ წარმოადგენს სწორ არჩევანს თქვენი ორგანიზაციისათვის. თუმცა, რამდენადაც VPN-ის გამოყენება უფრო საყოველთაო ხდება, ეს უფრო ნაკლებად განმასხვავებელი ფაქტორია. VPN-ის ყოველთვის ნაგულისხმევად გამოყენება წარმოადგენს საუკეთესო არჩევანს, თუ ეს მართლზომიერი და შესაძლებელია.

რომელ ბრაუზერს უნდა ვიყენებდეთ?

გამოიყენეთ ავტორიტეტული ბრაუზერი, როგორიცაა Chrome-ი, Firefox-ი, Brave-ი, Safari-ი, Edge-ი ან Tor Browser-ი. როგორც Chrome-ი, ისე Firefox-ი მეტად ფართოდ გამოიყენება და მშვენივრად მუშაობს უსაფრთხოების თვალსაზრისით. ზოგიერთი უპირატესობას Firefox-ს ანიჭებს კონფიდენციალურობაზე ორიენტირებულობის გამო. ნებისმიერ შემთხვევაში, მნიშვნელოვანია, რომ შედარებით ხშირად გადატვირთოთ ისინი და თქვენი კომპიუტერი თქვენი ბრაუზერის განახლების მიზნით. თუ დაინტერესებული ხართ ბრაუზერის ფუნქციების შედარებით, იხ. Freedom of the Press Foundation-ის ეს **რესურსი**. მიუხედავად ბრაუზერისა, ასევე კარგი აზრია გამოიყენოთ გაფართოება ან დამატება, როგორიცაა **Privacy Badger-ი**, **uBlock Origin-ი** ან **DuckDuckGo's Privacy Essentials-ი**, რომლებიც შეაჩერებს მეტოქეების და სხვა მესამე მხარის მოთვალთვალეების მიერ იმის აღრიცხვას, თუ სად წახვედით და რომელ ვებგვერდებს ეწვიეთ. ხოლო ინტერნეტში ბრაუზინგისას გადართეთ ქსელში თქვენი ნაგულისხმევი ძიება Google-დან **DuckDuckGo-ზე**, **Startpage-ზე** ან კონფიდენციალურობის დამცველ სხვა საძიებო სისტემაზე. ხსენებული გადართვა დაგეხმარებათ მეტოქეების და მესამე მხარის მოთვალთვალეების შეზღუდვაშიც.

ბრაუზინგის დაცულობა რეალურ სამყაროში

სამოქალაქო საზოგადოების ტიბეტელმა აქტივისტებმა განიცადეს **შეტევა** 2021 წ. დასაწყისში ჭკვიანურად მოფიქრებული ბრაუზერის საზიანო დანამატით, რომელმაც მოიპარა მათი ელ-ფოსტა და ბრაუზინგის მონაცემები. დანამატი, რომლის დასახელებაც „ფლეშის განახლების კომპონენტი" იყო, წარედგინა მომხმარებლებს, რომლებიც ეწვივნენ ფიშინგურ ელწერილებზე მიბმულ ვებსაიტებს. აღნიშნული ბრაუზერის გაფართოებით ან დანამატით შეტევები შესაძლოა ისევე დამაზიანებელი იყოს, როგორც საზიანო პროგრამა, გაზიარებული უშუალოდ ფიშინგური ჩამოტვირთვების ან სხვა პროგრამული უზრუნველყოფის საშუალებით.



სოციალური მედიის უსაფრთხოება

თქვენს ორგანიზაციას შეუძლია გაამჟღავნოს ბევრი რამ – და ხანდახან განზრახულზე მეტი – სოციალურ მედიაში პოსტების და კომენტარების საშუალებით.

იქნება ეს Facebook-ი, Twitter-ი, Instagram-ი, YouTube-ი თუ რეგიონისთვის დამახასიათებელი სოციალური მედიის ვებგვერდები, როგორიცაა Vkontakte-ი და Odnoklassniki-ი, მუდამ უნდა დაუფიქრდეთ რა პოსტს წერთ და აწარმოოთ უსაფრთხოების ყველა ხელმისაწვდომი პარამეტრის სწორი კონფიგურაცია. ეს მართებულია არა მხოლოდ თქვენი ორგანიზაციის ოფიციალური გვერდების, არამედ, ზოგიერთ შემთხვევაში, პერსონალის და მათი ოჯახების და მეგობრების პირადი პროფილებისათვისაც.

სოციალური მედიის უსაფრთხოება და სამოქალაქო საზოგადოება

უსაფრთხოების პოლიტიკის არქონის შემთხვევაში დაბალი რისკის მქონე ორგანიზაციაც კი შეიძლება გახდეს სოციალურ მედიაში თავდასხმის და დევნის ობიექტი. 2018 წ. მოცემულ მაგალითში, ცხოველების არაკომერციულმა თავშესაფარმა ათასობით დოლარი და მხარდამჭერი დაკარგა მას შემდეგ, რაც არაუფლებამოსილმა პროფილის ადმინისტრატორმა გამართა ფინანსების მოძიების ყალბი კამპანია, ხოლო პლატფორმაზე გამოჩნდნენ თანამშრომლებად თავის გამსაღებელი ყალბი პროფილები. თუ ჰაკერები იმ ზომამდე მივლენ, რომ იშოვონ რამდენიმე ათასი დოლარი ცხოველების თავშესაფრის დახმარებით, შეგიძლიათ წარმოიდგინოთ ზიანი, რომელიც შესაძლოა მოიტანონ მოხერხებულმა მეტოქეებმა, თუ მიიღებენ წვდომას თქვენი ორგანიზაციის პროფილებზე ან წარმატებულად გაასაღებენ თავს თქვენს ორგანიზაციად. გარდა პროფილების გატეხვისა, სამოქალაქო საზოგადოების ჯგუფები და ინდივიდუალური მომხმარებელი ასევე დგანან სოციალურ მედიაში გამოქვეყნებული კონტენტის შედეგების წინაშე მრავალ ქვეყანაში. მაგალითად, 2020 წ. ზამბიაში პოლიციამ დააპატიმრა 15 წლის მოსწავლე Facebook-ის პოსტში პრეზიდენტის ვითომ და ცილისწამების გამო. ბავშვი, რომელმაც პოსტი ფსევდონიმით გამოაქვეყნა, იდენტიფიცირებული იქნა სარეგისტრაციოდ გამოყენებული ტელეფონის ნომრით და მისი ინტერნეტ-პროტოკოლის (IP-ი) მისამართით.



სოციალური მედიის ორგანიზაციული პოლიტიკის შემუშავება

წარმოიდგინეთ, რომ ნებისმიერი პოსტი სოციალურ მედიაში შესაძლოა იქცეს საჯარო განცხადებად და შესაბამისად, შექმენით სოციალური მედიის ორგანიზაციული პოლიტიკა. ხსენებული უნდა პასუხობდეს შემდეგ კითხვებს: ვის აქვს წვდომა სოციალურ მედიაში თქვენს პროფილებზე? ვის აქვს უფლება გამოაქვეყნოს პოსტები და ვის ესაჭიროება პოსტების დადასტურება? რა ინფორმაცია უნდა/არ უნდა გაზიარდეს სოციალურ მედიაში? თუ აქვეყნებთ ფოტოებს, ლოკაციის შესახებ ინფორმაციას ან სხვა საიდენტიფიკაციო ინფორმაციას თქვენი პერსონალის, პარტნიორების ან ღონისძიებაზე დამსწრეთა შესახებ, სთხოვეთ მათ ნებართვა და გაითვალისწინეს მათ რისკები? გარდა თქვენი პოლიტიკის შემუშავების და მისი პერსონალისთვის განმარტებისა, უზრუნველყავით თქვენი კონფიდენციალურობის და დაცვის (ხშირად „უსაფრთხოებად“ ხსენებული) პარამეტრების სწორი კონფიგურაცია. ზოგიერთი საკვანძო კითხვა, რომელიც უნდა დაუსვათ საკუთარ თავს, რათა გადაწყვიტოთ კონფიდენციალურობის და უსაფრთხოების რომელი პარამეტრებია უმთავრესი თქვენი პირადი და ორგანიზაციული პროფილებისათვის, მოიცავს:

- საჯაროდ გსურთ, გააზიაროთ თქვენი პოსტები თუ მხოლოდ ადამიანთა კონკრეტულ შიდა ან გარე ჯგუფთან?
- უნდა შეეძლოს ვინმეს დაწეროს კომენტარი, პასუხი ან აწარმოოს ინტერაქცია თქვენს შეტყობინებებზე ან პოსტებზე?
- უნდა შეეძლოს ხალხს მოგძებნონ თქვენ ან თქვენი ორგანიზაცია თქვენი ელ-ფოსტის მისამართის ან ტელეფონის ნომრის გამოყენებით (პირადი თუ სამსახურეობრივი)?
- გსურთ თქვენი ლოკაციის გაზიარება ავტომატურად პოსტების წერისას?
- გსურთ დაბლოკოთ ან გამოურთოთ შეტყობინებები არაკეთილგანწყობილ პროფილებს?
- გსურთ დაბლოკოთ კონკრეტული სიტყვები ან ჰეშტეგები?

სოციალური მედიის თითოეულ ვებგვერდს გააჩნია კონფიდენციალურობის და უსაფრთხოების განსხვავებული პარამეტრები, თუმცა, ზოგადი კონცეფციები გავრცელებულია უნივერსალურად. აღნიშნული კითხვების შემდეგ ისარგებლეთ შემდეგი უმთავრესი პლატფორმების პრივატულობის შესახებ სახელმძღვანელოებით: **Facebook-ი**, **Twitter-ი**, **Instagram-ი** და **YouTube-ი**. კერძოდ, Facebook-თვის ყურადღება მიაქციეთ თქვენს კონფიდენციალურობის არჩევანს Groups-თან მიმართებაში. Facebook Groups პოპულარული ადგილია ჩართვის, მხარდაჭერის და ინფორმაციის გაზიარების თვალსაზრისით, თუმცა, შეუზღუდავ ჯგუფებს ყველა შესაძლოა შეუერთდეს. „ყალბი“ პროფილებისათვის ჩვეულებრივი ამბავია წარმოაჩინონ თავი რეალურ ადამიანებად, რათა შეაღწიონ დახურულ ჯგუფებში და გვერდებზე სოციალურ მედიაში. ამდენად, ყურადღებით იყავით „მეგობრობის“ და „გამოწერის“ შემოთავაზების დადასტურებისას. გახსოვდეთ, რომ თქვენი ორგანიზაციის პროფილები სოციალურ მედიაში დაცულია მხოლოდ იმდენად, რამდენადაც დაცულია მათთან „დაკავშირებული“ პროფილები. ეს განსაკუთრებით მნიშვნელოვანია გახსოვდეთ Facebook-ის შემთხვევაში, სადაც თქვენი ორგანიზაციის გვერდი შესაძლოა იმართებოდეს ვინმეს მიერ მიბმული პირადი პროფილიდან.

ონლაინ დევნა

სამწუხაროდ, არაერთი ორგანიზაცია განიცდის მნიშვნელოვან ონლაინ დევნას, განსაკუთრებით, სოციალურ მედიაში. აღნიშნული **დევნა ხშირად უფრო ძლიერია ქალების და მარგინალიზებული მოსახლეობის მიმართ.** კერძოდ, ონლაინ ძალადობამ ქალებზე შესაძლოა შექმნას მტრული გარემო, რომელიც იწვევს თვითცენზურას ან უარს პოლიტიკურ თუ სამოქალაქო დისკურსზე. თანახმად NDI-ს Gender, Women, and Democracy-ის ჯგუფის ანგარიშისა **Tweets that Chill**, როცა შეტევები პოლიტიკურად აქტიური ქალების წინააღმდეგ ხორციელდება ონლაინ, სოციალური მედიის ფართო წვდომამ შესაძლოა გაზარდოს დევნის და ფსიქოლოგიური ზეწოლის ეფექტი ხელყოფს რა ქალების პირადი უსაფრთხოების გრძნობას იმ საშუალებებით, რომლებსაც მამაკაცები არ განიცდიან.

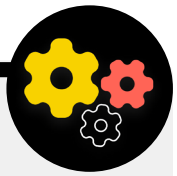
თქვენი ორგანიზაციის მიერ სოციალური მედიის პოლიტიკის შემუშავების შემდეგ მნიშვნელოვანია კარგად იცნობდეთ ხსენებულ დინამიკას. დანერგეთ უსაფრთხოების თქვენი გეგმა, რომლის მიზანია იმ პერსონალის მხარდაჭერა, რომელიც იღებს ნეგატიურ შეტყობინებებს, შეურაცხყოფას და მუქარას სოციალურ მედიაში გამომდინარე როგორც მათი სამსახურიდან, ისე პირადი ცხოვრებიდან. შეიმუშავეთ დევნის საწინააღმდეგო ინფრასტრუქტურა თქვენი ორგანიზაციის ფარგლებში, მათ შორის, აწარმოეთ საკუთარი პერსონალის კვლევა, რათა გაიგოთ როგორ მოქმედებს ონლაინ დევნა მათზე და შექმნათ სწრაფი რეაგირების ჯგუფი, რათა დაეხმაროთ პერსონალს დაძაბულ სიტუაციებში. PEN America-ის **„ონლაინ დევნის საველე სახელმძღვანელო“** ასევე იძლევა დეტალურ რეკომენდაციებს, თუ როგორ შეგიძლიათ დაეხმაროთ დევნის განმცდელ პერსონალს. თუ თქვენი პერსონალი კომფორტულად იგრძნობს თავს ამ პროცესში, შეგიძლიათ, დანერგოთ დევნის **შემთხვევებზე ინფორმირებისას** ან/და პრობლემურ ანგარიშებზე ინფორმირების (რეპორტინგის) პრაქტიკა უშუალოდ პლატფორმებთან.

იმ პერსონალთან ურთიერთობისას, რომელიც ონლაინ (თუ რეალურ სამყაროში) შევიწროების მსხვერპლი, მნიშვნელოვანია იყოთ მგრძნობიარე. თანახმად Association for Progressive Communications-ის Women’ s Rights Programme-ის **Take Back the Tech-ში** ხაზგასმულია, უნდა გესმოდეთ, რომ დაზარალებულს შესაძლოა მიეღო ტრავმა და აცნობიერებდეთ, რომ ძალადობა (ონლაინ თუ ოფლაინ) არასდროს წარმოადგენს დაზარალებულის ბრალს. უზრუნველყავით ასეთი პრობლემების წამოწევის და განხილვის შესაძლებლობა (თუ პერსონალს არა აქვს ამასთან რაიმე პრობლემა) კონფიდენციალურ და უსაფრთხო გარემოში ანონიმურობის დაცვის არჩევანთან ერთად. და შეიტანეთ თქვენი ორგანიზაციის უსაფრთხოების გეგმაში იმ ადგილობრივი პროფესიონალების, ორგანიზაციების და სამართალდამცველი უწყებების სია, რომლებსაც, საჭიროების შემთხვევაში, შეგიძლიათ დააკავშიროთ პერსონალი სამართლებრივი, სამედიცინო, ფსიქიკური და ტექნიკური დახმარების მისაღებად. დამატებითი ინფორმაციისათვის იხ. Feminist Frequency-ის **„ონლაინ უსაფრთხოების სახელმძღვანელო“**.

თქვენი ვებგვერდი ონლაინ რეჟიმში

გარდა ინტერნეტზე უსაფრთხო წვდომის თქვენი შესაძლებლობის დაცვისა, ასევე მნიშვნელოვანია ყველაფერი გააკეთოთ, რათა უზრუნველყოთ თქვენი ორგანიზაციის ვებგვერდებზე თუ რესურსებზე სხვების წვდომაც.

სოციალურ მედიაში გვერდებთან მიმართებაში, აღნიშნული გულისხმობს ხსენებული პროფილების დაცვას ძლიერი, უნიკალური პაროლებით და აუთენტურობის ორფაქტორული შემოწმებით. თქვენი ვებგვერდისათვის ეს გულისხმობს გატეხვისაგან მის დაცვას და სერვისზე შეტევების მოგერიებას. Distributed Denial of Service-ის (DDoS-ი) შეტევებს ადგილის აქვს, როცა კომპიუტერების დიდი ჯგუფი ერთდროულად ჩაითრევს თქვენს სერვერს საზიანო ტრაფიკში. თუ წარმოადგენთ სამოქალაქო საზოგადოებრივ ორგანიზაციას ან არაკომერციულ ორგანიზაციას, დიდი ალბათობით შეგიძლიათ უფასოდ მიიღოთ DDoS-გან დაცვა - რაც მეტად გაურთულებს მეტოქეს თქვენი ვებგვერდის გათიშვას. რამდენიმე ოფცია მოიცავს შემდეგ სერვისებს: Cloudflare-ის **Project Galileo-ი**, Google-ის **Project Shield-ი** ან eQualitie-ის **Deflect-ი**.



თქვენი ორგანიზაციის ვებგვერდის უსაფრთხო ჰოსტინგი

ვებგვერდები განთავსებულია კომპიუტერებში - ისინი კი მოწყვლადია ჰაკერების მიმართ ზუსტად ისე, როგორც თქვენი საკუთარი მოწყობილობები. თუ შესაძლებელია, თქვენმა ორგანიზაციამ უნდა ისარგებლოს არსებული ჰოსტინგ-სერვისებით, როგორიცაა Wordpress.com-ი, Wix-ი ან სხვები, რომლებიც წარმართავენ გვერდის უსაფრთხოების ყველა საკითხს თქვენს მაგივრად. თუ კითხულობთ წინამდებარე სახელმძღვანელოს, თქვენს ორგანიზაციას, სავარაუდოდ, ასევე უფლება აქვს მიიღოს Wordpress-ის უფასო და უსაფრთხო ჰოსტინგი **eQualitie-ზე** მათი **eQPress Hosting service-ის**აშუალებით. ეს მშვენიერი ოფციაა Wordpress-ის არსებული გვერდებით მოსარგებლე სამოქალაქო ორგანიზაციებისათვის ან თუ თქვენს ორგანიზაციას განზრახული აქვს შექმნას ახალი გვერდი. თუ თქვენი ვებგვერდის საჭიროებები უფრო კომპლექსურია ან თუ გესაჭიროებათ თქვენი ვებგვერდის თავად ჰოსტინგი, კონცენტრაცია მოახდინეთ თქვენი ოპერაციული სისტემის და ვებ-ჰოსტინგის პროგრამული უზრუნველყოფის მუდმივ განახლებაზე ზუსტად ისე, როგორც თქვენი პერსონალური კომპიუტერის შემთხვევაში. გაითვალისწინეთ აღიარებული ქლაუდ-ჰოსტინგის იმ პროვაიდერების გამოყენება, როგორიცაა Amazon Web Services-ი (AWS-ი), Microsoft Azure-ი ან Greenhost-ის **eclips.is-ი**, რომლებიც გვთავაზობენ უსაფრთხოების გაძლიერებულ ოფციებს მათ ჰოსტინგს დაქვემდებარებული ვებგვერდებისათვის. მიუხედავად იმისა, თუ რომელ ინსტრუმენტებს იყენებთ თქვენი ვებგვერდის ჰოსტინგისათვის, უზრუნველყავით, რომ კონტენტის რედაქტირებაზე წვდომის მქონე ნებისმიერი პროფილი და კონფიგურაციის პარამეტრები დაცული იყოს ძლიერი პაროლებით და აუთენტურობის ორფაქტორული შემოწმებით.

თუ თქვენი ორგანიზაცია საკმარისად ტექნიკასთან-მეგობრულია საკუთარი ვებგვერდის ჰოსტინგისთვის შესაძლებლობისთვის, იფიქრეთ ე.წ. „სტაციონარული საიტის“ ან არასტრუქტურული ვებგვერდის არჩევაზე. განსხვავებით დინამიკური ვებგვერდებისაგან, აღნიშნული ტიპის საიტები უმცირებს ჰაკერებს შეტევის ნიადაგს და შეტევებისადმი უფრო მდგრადს ხდის თქვენს ვებგვერდს.

დაიცავით თქვენი WiFi ქსელი

ყველა აღნიშნული ნაბიჯი ვებ-ტრაფიკის თვალთვალის და ცენზურისაგან დასაცავად მნიშვნელოვანია, თუმცა, ისინი არ წარმოადგენს ოფისში და სახლში საბაზისო ქსელის უსაფრთხოების ალტერნატივას.

არ დაგავიწყდეთ საფუძვლები, როგორიცაა ძლიერი პაროლის (და არა უბრალო პაროლის) გამოყენება თქვენს WiFi-ის რუტერზე (რუტერებზე), რაც უზრუნველყოფს თქვენს ქსელზე მხოლოდ უფლებამოსილი მომხმარებლის წვდომას ხშირად ცვლადი პაროლით და თქვენი უსადენო რუტერების საკუთარი ქსელთაშორისი ეკრანის ამუშავება. ასევე, განიხილეთ თქვენს ოფისში სტუმრებისთვის განკუთვნილი ქსელის დაყენებაზე, თუ გყავთ ვიზიტორები, რომლებიც შემოდიან და გადიან შენობიდან და იყენებენ ინტერნეტს.

უსაფრთხოების დაცვა ინტერნეტში

- **აწარმოეთ პერსონალის რეგულარული ტრენინგი ვებ-უსაფრთხოების ღონისძიებების განხორციელების მნიშვნელობის საკითხებზე.**
- **შეახსენეთ პერსონალს მუდამ აწარმოოს ბრაუზინგი HTTPS-ით და დაშიფრული DNS-ით.**
- **მოსთხოვეთ პერსონალს რეგულარულად გადატვირთოს მისი ბრაუზერები განახლებების ინსტალაციისათვის.**
- **წაახალისეთ კონფიდენციალურობის დამცველი ბრაუზერების და გაფართოებების გამოყენება.**
- **თუ VPN-ი შესაფერისია თქვენი ორგანიზაციის კონტექსტში, აირჩიეთ კარგი რეპუტაციის მქონე, აწარმოეთ პერსონალის ტრენინგი მისი გამოყენების საკითხებზე და უზრუნველყავით მისი მუდმივი გამოყენება.**
- **შეიმუშავეთ და გაავრცელეთ ნათელი ორგანიზაციული პოლიტიკა სოციალური მედიის გამოყენების შესახებ.**
- **ჩართეთ კონფიდენციალურობის და უსაფრთხოების პარამეტრები სოციალური მედიის ყველა პროფილში.**
- **გააცნობიერეთ ონლაინ დევნის გავლენა და მზად იყავით მხარი დაუჭიროთ შევიწროებულ პერსონალს.**
- **შეიმუშავეთ იმ ადგილობრივი პროფესიონალების, ორგანიზაციების და სამართალდამცველი უწყებების სია, რომლებსაც, საჭიროების შემთხვევაში, შეგიძლიათ დააკავშიროთ პერსონალი სამართლებრივი, ფსიქიკური და ტექნიკური დახმარების მისაღებად ონლაინ დევნის პასუხად.**
- **გამოიწერეთ DDOS-ის დაცვა თქვენი ვებგვერდისათვის.**
- **გამოიყენეთ ვებ-ჰოსტინგის სანდო, საიმედო პროვაიდერი.**
- **გამოიყენეთ ძლიერი პაროლი და სტუმრის ქსელი თქვენი ოფისის WiFi-თვის.**



ფიზიკური უსაფრთხოების დაცვა

მნიშვნელოვანია ფიზიკურად დაცულ ადგილას შეინახოთ თქვენი მოწყობილობები. გახსოვდეთ, რომ ფიზიკური უსაფრთხოება სცილდება უბრალოდ მოწყობილობებს და უნდა მოიცავდეს სტრატეგიას დაიცვათ ყველაფერი დანარჩენი თქვენს სამყაროში. აღნიშნული მოიცავს ნაბეჭდ დოკუმენტებს; თქვენი ორგანიზაციის ოფისს თუ სამუშაო სივრცეებს; და, რა თქმა უნდა, თქვენს პერსონალს და მოხალისეებს.

თვალთვალი, ცენზურა და სამოქალაქო საზოგადოება

სამწუხაროდ, ფიზიკური თავდასხმები სამოქალაქო საზოგადოებრივი ორგანიზაციებზე არაა იშვიათი და ხშირად მნიშვნელოვანი ზეგავლენა აქვს როგორც ფიზიკური, ისე ინფორმაციული უსაფრთხოების თვალსაზრისით. მეტოქეების მიერ გამოყენებული ერთი საერთო ტაქტიკა CSO-ების საქმიანობის ჩასახშობად მოიცავს ოფისებში შეჭრას და დახურვას - პერსონალის როგორც დაშინებას, ისე, ზოგიერთ შემთხვევაში, ინფორმაციის და ტექნიკური აღჭურვილობის ქურდობას ან კონფისკაციას. ხსენებული საფრთხეები ხშირად მიმართულია უმცირესობების და ადამიანის უფლებების დამცველი ჯგუფების და დემოკრატიის და მმართველობის სივრცეში მომუშავე CSO-ების წინააღმდეგ. მაგალითად, LGBT+ Rights Ghana განას (სამოქალაქო ორგანიზაცია, რომელმაც 2021 წ. დასაწყისში ქვეყანაში გახსნა პირველი საზოგადოებრივი ცენტრი LGBTQI+ საზოგადოებისათვის) ოფისებში მიიღეს დაწვის მუქარა, [საბოლოოდ კი მათ პოლიცია დაესხა თავს და დახურა ისინი]. ამგვარი თავდასხმები მოქმედებს არა მხოლოდ ორგანიზაციის ფიზიკურ ოპერაციებზე, არამედ შესაძლოა დაუკარგოს პერსონალს უსაფრთხოების გრძნობაც.

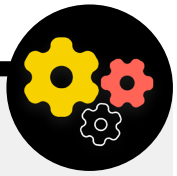


ფიზიკური აქტივების დაცვა

ინფორმაციის დაცვის უმნიშვნელოვანესი კომპონენტია მოწყობილობების ფიზიკური უსაფრთხოება.

გარდა მოწყობილობის ქურდობით გამოწვეული ზეგავლების შესუსტებისა ეკრანის ბლოკირების და პაროლების გამოყენებით, დისკის სრულად დაშიფვრით და დისტანციური წაშლის ფუნქციის ჩართვით, უპირველეს ყოვლისა, ასევე უნდა იფიქროთ როგორც დაიცვათ ხსენებული მოწყობილობები ქურდობისაგან. ქურდობის გასართულებლად, დაამონტაჟეთ შეუვალი საკეტები (და ცვალეთ ისინი პერსონალის შეცვლისას) ოფისში ან/და სახლში. გარდა ამისა, იფიქრეთ ლეპტოპის სეიფის ან ჩასაკეტი კარადის ყიდვაზე მოწყობილობების ღამით დასაცავად. უსაფრთხოების კამერები მნიშვნელოვნად გაიაფდა და მათი სახლში გამოსაყენებელი მარტივი ვარიანტები უფრო ფართოდაა ხელმისაწვდომი. აღნიშნულმა კამერამ ან მოძრაობის სენსორულმა სისტემამ სათავსოების გარშემო შესაძლოა დააფიქსიროს და შეაჩეროს ფიზიკური შეჭრა და ქურდობა. ნახეთ თქვენს ქვეყანაში ხელმისაწვდომი კონფიდენციალურობის დამცავი ოფცია და უცილობლად აირჩიეთ იმ სანდო კომპანიების მიერ შემოთავაზებული კამერები, რომლებსაც არა აქვთ ინტერესი, გადასცენ მონაცემები და ინფორმაცია პოტენციურ მეტოქეს.

თუ შემოჭრის ან ოფისზე თავდასხმის რისკი მაღალია, შეინახეთ ორგანიზაციის ყველაზე სენსიტიური მონაცემები ოფისს გარეთ ქლაუდზე უსაფრთხოდ შენახვით (როგორც განხილულია ზემოთ) ან თავდასხმის ნაკლებად შესაძლო ადგილზე ფიზიკური გადატანით. თუ ძველ მოწყობილობებზე არის ინფორმაცია, რომელიც ჯერაც დაცულია მათზე, თუმცა, აღარ გამოიყენება, იფიქრეთ მის წაშლაზე - Wirecutter-ის მოცემული სახელმძღვანელო შესანიშნავი რესურსია იმისა, თუ როგორ უნდა გაკეთდეს ეს თანამედროვე მოწყობილობების უმეტესობაში. თუ თქვენი აპარატების წაშლა შეუძლებელია, შეგიძლიათ ფიზიკურად გაანადგუროთ ისინი. ამისათვის უმარტივესი, თუმცა გარემოს დაცვის თვალსაზრისით არასასურველი გზაა მოწყობილობების დამტვრევა და მათი მყარი დისკების ჩაქუჩით დამსხვრევა. ხანდახან ძველი მეთოდი ჯერაც საუკეთესოა! ხსენებული ტექნიკური ნაბიჯების წინაც კი დაუთმეთ დრო ორგანიზაციის მთელი აღჭურვილობის ინვენტარიზაციას. თუ არ გაქვთ ყველა თქვენი მოწყობილობის სია, უფრო რთულია იმის აღრიცხვა, თუ რა დაგაკლდათ ერთ-ერთის ქურდობის შემთხვევაში.



თქვენი საკუთარი ოფისის დაცვის სისტემის გამართვა

თუ ოფისის სრულად დაცვის სისტემა ვერ დაიფარება თქვენი ორგანიზაციის ბიუჯეტით და განსაკუთრებით შეშფოთებული ხართ კონფიდენციალურობის საკითხთან დაკავშირებით, შეგიძლიათ სცადოთ კრეატიული ოფცია, როგორიცაა Guardian პროექტის აპი Haven-ი, რომელიც გაცნობებთ ოფისში შესაძლო შეჭრის შესახებ. Haven-ი წარმოადგენს სმარტფონის აპს, რომელსაც შეუძლია აქციოს ნებისმიერი ანდროიდის ტელეფონი მოძრაობის, ხმაურის, ვიბრაციის და სინათლის დეტექტორად. შეგიძლიათ გამართოთ აპი რამდენიმე იაფ ანდროიდის მოწყობილობაზე ოფისის სხვადასხვა წერტილში, რათა გეცნობოთ და დააფიქსიროთ ნებისმიერი მოულოდნელი და არასასურველი ვიზიტორი. აპი Haven-ი შესაძლოა ასევე სასარგებლო იყოს სასტუმროს ნომერში ან ბინაში დამონტაჟებით, თუ განიცდით მომეტებულ რისკს. ყველაზე კარგია სრული უსაფრთხოების სისტემა, თუმცა, თუ ის არაა ხელმისაწვდომი და გსურთ მეტის შეტყობა, თუ როგორ გამოიყენოთ აპი Haven-ი, შეგიძლიათ ეწვიოთ პროექტის ვებგვერდს.

რა ვუყოთ ამდენ ქაღალდს?

არსებობს დიდი ალბათობა, რომ თქვენს ორგანიზაციას გააჩნდეს დიდი ოდენობით ინფორმაცია, რომელიც დაბეჭდილია ქაღალდზე, ჩაწერილია ბლოკნოტებში ან ჩანიშნულია სტიკერებზე. ზოგიერთი მათგანი შესაძლოა მეტად საფრთხილო იყოს: ბიუჯეტის ამონაბეჭდები, მონაწილეების სიები, სენსიტიური წერილები დონორებისაგან და შენიშვნები კონფიდენციალური შეტყობინებებიდან. ასევე მნიშვნელოვანია გვახსოვდეს ხსენებული ინფორმაციის უსაფრთხოება. თუ აუცილებლად გესაჭიროებათ სენსიტიური ინფორმაციის ამონაბეჭდი ასლების შენახვა, უზრუნველყავით, რომ ის უსაფრთხოდ ინახებოდეს ჩაკეტილ კარადაში ან სხვა დაცულ ადგილას. ნუ დატოვებთ რაიმე პრივატულ ან სენსიტიურ ინფორმაციას (მათ შორის, პაროლებს) მაგიდაზე მიმოფანტულს ან ჩაწერილს პრეზენტაციების დაფაზე. თუ მიგაჩნიათ, რომ თქვენი ორგანიზაცია განიცდის შეჭრის ან თავდასხმის დიდ რისკს, შეინახეთ მნიშვნელოვნად სენსიტიური ინფორმაცია თავდასხმის ნაკლებად მოსალოდნელ ადგილზე. რამდენადაც შესაძლებელია, ეცადეთ მოიცილოთ არასაჭირო ინფორმაციის ამონაბეჭდები. გახსოვდეთ: შეუძლებელია იმის მოპარვა, რაც არ გაქვთ. დააწესეთ ორგანიზაციული პოლიტიკა ამონაბეჭდ შენიშვნებზე პასუხისმგებელი პირის შესახებ და უზრუნველყავით მთელი პერსონალისაგან ნებისმიერი ფურცლის ამოღება, თუ ისინი თავიანთი ან ორგანიზაციის გადაწყვეტილების საფუძველზე, დატოვებენ ორგანიზაციას, დაიბრუნეთ ნაბეჭდი ინფორმაცია მათგან (ზუსტად ისე, როგორც ამოიღებდით ორგანიზაციის მიერ გაცემულ კომპიუტერს ან) ტელეფონს. თავიდან მოიცილეთ სენსიტიური ქაღალდები, რისთვისაც შეიძენთ ხარისხიან ქაღალდსაჭრელს. თქვენს პერსონალთან კვირის ბოლოს ღონისძიებას შესაძლოა 15 წუთიანი შესვენება დასჭირდეს, რათა ქაღალდის საჭრელში გაანადგუროთ გასული კვირის ნებისმიერი ნარჩენი და ამონაბეჭდი სენსიტიური შენიშვნა.

ოფისის პოლიტიკა

მიუხედავად იმისა, რომ COVID-19-ის პანდემიის დაწყების შემდეგ მნიშვნელოვნად შეიცვალა მრავალი „საოფისე“ წესი, თქვენი ორგანიზაციისათვის კვლავ მნიშვნელოვანია გააჩნდეს ნათელი პოლიტიკა ოფისში დაშვების შესახებ. ხსენებული პოლიტიკით უნდა გადაწყდეს საკვანძო საკითხები, მათ შორის, თუ ვინ და როდის არის დაშვებული ოფისში, ვის აქვს წვდომა ოფისის რესურსებზე (მაგ. WiFi ქსელზე) და რომელ მათგანზე და როგორ მოიქცეთ სტუმრებთან მიმართებაში.

მარტივი, თუმცა მნიშვნელოვანი კითხვაა ვის უნდა ჰქონდეს ოფისის გასაღები. გასაღები უნდა ჰქონდეს მხოლოდ სანდო პერსონალს, ხოლო საკეტები უნდა იცვლებოდეს, როცა პერსონალი მიდის ან/და გარკვეული პერიოდულობით. დღის განმავლობაში, ყველა ჩაუკეტავი კარი უნდა იყოს ორგანიზაციისათვის სანდო პირის მხედველობის არეში. ასევე დაფიქრდით სანდო ურთიერთობა აქვს თუ არა ორგანიზაციას ოფისის გამქირავებელთან თუ დამლაგებლებთან. იფიქრეთ რომელ ინფორმაციაზე ან მოწყობილობაზე გააჩნია წვდომა ამ ხალხს და უზრუნველყავით მათი დაცვა, განსაკუთრებით, თუ სანდო ურთიერთობა არ გაქვთ. ვისაც არ უნდა გააჩნდეს წვდომა, ვინმე სანდო მუდმივად უნდა იყოს გამოყოფილი ოფისზე ზედამხედველობისთვის, ასევე, უზრუნველყავით მოწყობილობების სწორად დაცვა დღის ბოლოს გასვლამდე.

დაიშვებიან ოფისში სტუმრები? თუ ასეა, უზრუნველყავით, რომ მათ არ გააჩნდეთ წვდომა (ან, სულ მცირე, უკონტროლო წვდომა) მოწყობილობებზე ან სენსიტიური მონაცემების ამონაბეჭდებზე. თუ არსებობს საჭიროება ან მოლოდინი, რომ სტუმრებს ვიზიტისას ექნებათ წვდომა ინტერნეტზე, უნდა გამართოთ „სტუმრის“ ქსელი ისე, რომ ხსენებულ სტუმრებს არ შეეძლოთ თქვენი რეგულარული ტრაფიკის მონიტორინგი. ზოგადად, ქსელზე და ქსელის მოწყობილობებზე, როგორიცაა პრინტერები, წვდომა უნდა გააჩნდეს მხოლოდ სანდო პერსონალს. ჩვეულებრივ, ასევე კარგი აზრია მოსთხოვოთ სტუმარს რეგისტრაცია ისე, რომ აწარმოოთ მომსვლელების ჟურნალი.

ოფისის პოლიტიკის შემუშავების მიზანი უნდა იყოს, რომ სენსიტიურ მოწყობილობებზე, დოკუმენტებზე, სივრცეებზე და სისტემებზე წვდომა შეეძლოთ მხოლოდ სანდო ადამიანებს.

დამხმარე პერსონალი და მოხალისეები

თქვენი ორგანიზაციის ფიზიკური უსაფრთხოების საფრთხეებმა შესაძლოა გავლენა იქონიოს თქვენს პერსონალზეც. სოციალურ ქსელებში დევნის მსგავსად, ფიზიკური უსაფრთხოების ხსენებული საფრთხეები ხშირად არაპროპორციულად მოქმედებს ქალებზე და მარგინალიზებულ საზოგადოებაზე. ეს არაა უბრალოდ გატეხილი ფანჯრები და მოპარული ლეპტოპები. ფიზიკური თუ სექსუალური ძალადობის მუქარამ, საფრთხეებმა თუ შემთხვევებმა, ოჯახურმა ძალადობამ და თავდასხმის შიშმა შესაძლოა სერიოზული ნეგატიური გავლენა იქონიოს პერსონალის ცხოვრებაზე. ორგანიზაციებისათვის, რომლებიც მუშაობს პოლიტიკურად აქტიურ ქალებთან ან მხარს უჭერს მათ, NDI-ს **#Think10-ის** Safety Planning Tool-ი შესაძლოა სასარგებლო რესურსი იყოს მათთვის მისაწოდებლად, ვინც შესაძლოა განიცდიდეს მომატებულ რისკს საკუთარი საქმიანობის შედეგად.

პერსონალის კეთილდღეობა აშკარად მნიშვნელოვანი აქტივია თავად მათთვის, როგორც პიროვნებებისათვის, თუმცა, ეს ასევე კრიტიკული ელემენტია ჯანსაღი და კარგად მომუშავე ორგანიზაციისათვისაც. ამ მიმართებაში, იფიქრეთ რა დამატებითი რესურსებით შეგიძლიათ უზრუნველყოთ პერსონალი მათ დასაცავად და, ფიზიკური თუ ციფრული თავდასხმის შემთხვევაში, მათი რეაბილიტაციის მიზნით. როგორც ზემოთ აღინიშნა წინამდებარე სახელმძღვანელოში, აღნიშნული გულისხმობს, სულ მცირე, იმ რესურსების სიის შედგენას, რომლებსაც, საჭიროების შემთხვევაში, შეგიძლიათ დააკავშიროთ პერსონალი სამართლებრივი, სამედიცინო, ფსიქიკური და ტექნიკური დახმარების მისაღებად. კიდევ ერთხელ, PEN America-ის **„ონლაინ დევნის საველე სახელმძღვანელო“** მოიცავს იდეებს, თუ როგორ შეუძლიათ ორგანიზაციებს მხარი დაუჭირონ პერსონალს კრიზისის დროს და მის შემდეგ, ხოლო Tactical Tech-ის **„თვალთვალისაგან თავდაცვის სახელმძღვანელო“** მოიცავს შესაბამის კონტენტს, თუ როგორ რეაგირებენ ხშირად ორგანიზაციები ინტენსიური საფრთხის დროს.

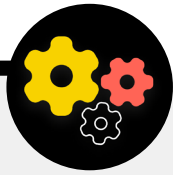
უსაფრთხოება მოგზაურობისას

მოგზაურობა - როგორც სხვა ქვეყანაში, ისე ქალაქიდან ქალაქში - ხშირად ზრდის ინფორმაციის ფიზიკური უსაფრთხოების რისკებს. ჩვეულებრივ უნდა დაუშვათ, რომ თქვენ და თქვენს მოწყობილობებს არ გაქვთ კონფიდენციალურობის უფლებები საზღვრების გადაკვეთისას. როგორც ასეთი, კარგი აზრია, ჩართოთ მოგზაურობის ორგანიზაციული პოლიტიკა უსაფრთხოების თქვენს გეგმაში, რომელიც მოიცავს შეხსენებას უსაფრთხოების აღიარებულ საკვანძო მეთოდებზე. თქვენი ორგანიზაციის მოგზაურობის პოლიტიკა უნდა მოიცავდეს სახელმძღვანელოს სხვა სექციებში მოცემულ მრავალ ინფორმაციას, მათ შორის, ინტერნეტის უსაფრთხოდ გამოყენებას და მოწყობილობების და სხვა ინფორმაციული წყაროების ფიზიკურ დაცვას თქვენი ნებისმიერი მოგზაურობის განმავლობაში. თუ შესაძლებელია, დატოვეთ თქვენი სენსიტიური ინფორმაცია და გამოიყენეთ ახალი, გაწმენდილი კომპიუტერი, გახსენით აუცილებლად საჭირო ფაილები ქლაუდიდან და შემდეგ წაშალეთ ის სახლში დაბრუნებისას.

გარდა მოგზაურობისათვის მომზადების და მოგზაურობისას თქვენს მიერ გაზიარებული მონაცემების მინიმიზაციისა, არსებობს რამდენიმე უმნიშვნელოვანესი ოპერაციული რჩევა, რომლებიც უნდა გაიაზროთ და ჩართოთ თქვენს მოგზაურობის ორგანიზაციულ პოლიტიკაში.

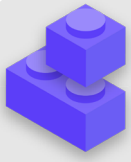
იფიქრეთ სპეციალური სამოგზაურო ლეპტოპების ან ტელეფონების გამოყენებაზე, რომლებშიც თითქმის არაა შენახული სენსიტიური ინფორმაცია. თუ თქვენი ორგანიზაციის სამუშაოს უმეტესობა სრულდება ქლაუდზე, შედარებით იაფი Chromebook-ი შესაძლოა კარგი არჩევანი იყოს ამგვარ მოწყობილობად. დაბრუნების შემდეგ აწარმოეთ ქარხნულ პარამეტრებზე დაბრუნება ან „ამოშლა" ამ მოწყობილობებში სახლში ან ოფისში ჩვეულ WiFi ქსელებში ჩართვამდე.
მოამზადეთ პერსონალი იმისათვის, თუ რა უნდა გააკეთოს, თუ იკითხებიან უწყებების მიერ ან შეაჩერებენ საზღვრის გადაკვეთისას. მოიფიქრეთ როგორ შეგიძლიათ შეზღუდოთ იმ ინფორმაციის რაოდენობა, რომელიც თან აქვს ვინმეს მოგზაურობისას, თუ ეს პრობლემაა, და შეიმუშავეთ შესახლების პროტოკოლები სენსიტიურ რეგიონებში მოგზაური პერსონალისათვის. მიაწოდეთ პერსონალს საკონტაქტო ინფორმაცია და სამოქმედო გეგმა მასზედ, თუ როგორ უნდა მოიქცნენ, თუ რაიმე პრობლემა შეიქმნება მათი მოგზაურობისას. აღნიშნული მოიცავს ინფორმაციას ადგილობრივი საავადმყოფოების, კლინიკების თუ აფთიაქების შესახებ, თუ დასჭირდებათ სამედიცინო დახმარება მოგზაურობისას.

პერსონალი ასევე ვალდებულია თან იქონიოს ყველა მოწყობილობა მოგზაურობისას. მაგალითად, ავტობუსში, მატარებელში და თვითმფრინავში შეინახეთ თქვენი ლეპტოპი ფეხებთან (და არა ზედა საბარგო თაროზე ან შემოწმებულ ბარგში). არ იფიქროთ, რომ სასტუმროს ნომერი – ან სასტუმროს სეიფიც კი – არის „უსაფრთხო ადგილი" სენსიტიური მოწყობილობის და საგნის შესანახად. ნუ ენდობით საჯარო USB-ის დასატენ პორტებს. USB-ის დასატენი პორტები აეროპორტებში, სადგურებზე და ტრანსპორტში სულ უფრო მეტ ყურადღებას იპყრობს და მეტად მოხერხებულია მოწყობილობების დასატენად. თუმცა, ისინი შესაძლოა საზიანო პროგრამის აკიდების მარტივ ვექტორად იქცეს. ამდენად, აუცილებლად დატენეთ მოწყობილობები ტრადიციული საშუალებით კედელში როზეტიდან ან შეიძინეთ **USB-ის მონაცემთა ბლოკები**, რათა მოგზაურ პერსონალს საშუალება ჰქონდეს უსაფრთხოდ დატენოს საკუთარი მოწყობილობები USB-ის საშუალებით.



უსაფრთხო მოგზაურობის დაჯავშნა თქვენი ორგანიზაციისათვის

მოგზაურობის პოლიტიკის ჩამოყალიბებისას, გახსოვდეთ, თუ რომელი ინფორმაცია შესაძლოა, იქნეს გაცხადებული მოგზაურობის ორგანიზების თუ დაჯავშნისას. კერძოდ, ეს შესაძლოა მნიშვნელოვანი იყოს, თუ ორგანიზებას უწევთ დიდ ღონისძიებას, ტრენინგს ან კონფერენციას, რომლისთვისაც იღებთ სენსიტიურ ინფორმაციას პერსონალის, პარტნიორების და/ან დამსწრეებისაგან. ყურადღებით დაფიქრდით, თუ უსაფრთხოდ როგორ გააზიარებთ და შეინახავთ (საჭიროების შემთხვევაში) პირად ინფორმაციას, როგორიცაა საპასპორტო რეკვიზიტები, მოგზაურობის მარშრუტები და სამედიცინო დოკუმენტები. Tactical Tech-ის Organizer Activity Book-ს გააჩნია შესანიშნავი უწყისი, რომელიც დაეხმარება თქვენს ორგანიზაციას დაფიქრდეს მოგზაურობის უსაფრთხოების საკვანძო საკითხებზე, **რომელზე ბმულიც მოცემულია აქ**.



თქვენი ფიზიკური უსაფრთხოების დაცვა

- **შეახსენეთ პერსონალს მუდამ ფიზიკურად დაცული იქონიოს მოწყობილობები.**
- **შეამოწმეთ და დაიცავით ყველა საშუალება, რომლითაც ხალხმა შესაძლოა შემოაღწიოს თქვენს სივრცეში - კარები და ფანჯრები.**
- **შეიმუშავეთ ოფისის სტუმრის და დაშვების პოლიტიკა.**
- **გამოიყენეთ შეუვალი საკეტები და დააბრუნეთ/ცვალეთ ისინი საჭიროებისამებრ.**
- **დაფიქრდით კამერების ან ოფისის სხვა უსაფრთხოების სისტემის დაყენებაზე.**
- **იქონიეთ და გამოიყენეთ ქაღალდის საჭრელი.**
  - გამოუყავით სპეციალური დრო პერსონალს იმ ამონაბეჭდი დოკუმენტების გასანადგურებლად, რომლებიც შეიცავს სენსიტიურ ინფორმაციას.
- **შეიმუშავეთ იმ ადგილობრივი პროფესიონალების, ორგანიზაციების და სამართალდამცველი უწყებების სია, რომლებსაც, საჭიროების შემთხვევაში, შეგიძლიათ დააკავშიროთ პერსონალი სამართლებრივი, სამედიცინო და ფსიქიკური დახმარების მისაღებად ფიზიკური თავდასხმის თუ საფრთხეების პასუხად.**
- **შეიმუშავეთ სამოგზაურო ორგანიზაციული პოლიტიკა.**
- **უზრუნველყავით, რომ პერსონალმა იცოდეს რა გააკეთოს ექსტრემალურ პირობებში მოგზაურობისას, მათ შორის, მოამზადეთ პერსონალი მასზედ, თუ როგორ მოიქცეს საზღვარზე ან ბლოკ-პოსტზე შეჩერებისას.**
- **ნებისმიერი ადგილობრივი, ქვეყნის ფარგლებში თუ საზღვარგარეთ მოგზაურობის წინ შეახსენეთ პერსონალს შეზღუდოს მოწყობილობებში შენახული ინფორმაციის რაოდენობა.**
- **არ დაგავიწყდეთ დამატებითი მონაცემები, რომლებიც იქმნება და გაზიარდება მოგზაურობის თუ ღონისძიებების ორგანიზებისას.**



როგორ იქცევით, როცა საქმე ცუდადაა

ამგვარად, იცით როგორ უნდა მოიქცეთ სწორად. უნდა დანერგოთ პოლიტიკები და აწარმოოთ ორგანიზაციაში ყველას ტრენინგი ყველა აღიარებული პრაქტიკის საკითხებზე. მიუხედავად ხსენებული რთული საქმისა, მეტად სავარაუდოა, რომ საბოლოოდ რაღაც არასწორად მოხდება.

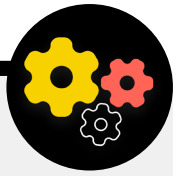
ხდება. ამ დროს, უმნიშვნელოვანესია დანერგილი იყოს შემთხვევაზე რეაგირების გეგმა. შემთხვევაზე რეაგირება თქვენი ორგანიზაციის უსაფრთხოების გეგმის კრიტიკული, და ხშირად არასაკმარისად დაფასებელი ნაწილია, რადგან შესაძლოა არსებობდეს სხვაობა თქვენი ორგანიზაციის რეპუტაციის დამანგრეველ შეტევას და გზაზე უსიამოვნო დარტყმას შორის. გახსოვდეთ, რომ შემთხვევაზე რეაგირება შეგიძლიათ მხოლოდ მაშინ, როცა იცით მის შესახებ. მაღალი ორგანიზაციული უსაფრთხოების კულტურის არსებობა და პერსონალის წახალისება განაცხადოს პრობლემების შესახებ მეტად მნიშვნელოვანია. ამიტომაა უკეთესი დაჯილდოვდეს უსაფრთხოების თვალსაზრისით სწორი ქცევა, ვიდრე დაისჯოს ნაკლოვანებები თუ შეცდომები. ასე მნიშვნელოვანია გამოიხატოს ემპათია და შემოწმდეს პერსონალის კეთილდღეობა მათ მიერ ინციდენტის შეტყობინების შესახებ. ასევე, პერსონალმა დაუყოვნებლივ უნდა გაცნობოთ ფიშინგურ შეტყობინებაში დაწკაპუნებული ბმულის, მოპარული ტელეფონის თუ სოციალურ მედიაში გატეხილი პროფილის შესახებ - ნუ იყოყმანებთ ანგარიშსწორების შიშის ან მხარდაჭერის ნაკლებობის გამო. საბოლოო ჯამში, ინციდენტზე რეაგირება ზუსტად ისე, როგორც წინამდებარე „სახელმძღვანელოს“ სხვა სექციებში განხილული შესუსტების სტრატეგიები, წარმოადგენს ორგანიზაციული დონის ძალისხმევას.

- რისთვის უნდა ემზადოთ? ერთი სიტყვით, ყველაფრისთვის, რაც კი შესაძლოა მოხდეს. აღნიშნული განსხვავებული იქნება თითოეული ორგანიზაციისათვის, თუმცა, საერთო კითხვები, რომლებზე პასუხშიც დაგეხმარებათ ინციდენტზე რეაგირების გეგმა, მოიცავს:
- როგორ ვიქცევით, თუ გატეხეს ჩვენი პროფილები ან ვებგვერდი?
- როგორ ვიქცევით, თუ ვინმე დააწკაპუნებს ფიშინგურ ელ-შეტყობინებაზე ან თუ მოწყობილობა იქცევა საეჭვოდ?
- როგორ ვიქცევით, თუ ჩვენი ელ-შეტყობინებები ან სენსიტიური დოკუმენტების უმეტესობა მოიპარეს და გამჟღავნდა?
- როგორ ვიქცევით, თუ ერთ-ერთი ჩვენი დასაქმებული მოხვდა ფიზიკურ საფრთხეში ან დააკავეს? ან თუ ისინი ებრძვიან სტრესს და მოუსვენრობას ხსენებული საფრთხეების გამო?
- როგორ ვიქცევით, თუ ოფისი დაზიანდა ხანძრის, წყალდიდობის ან სტიქიური უბედურების დროს?
- როგორ ვიქცევით, თუ თანამშრომლის კომპიუტერი ან ტელეფონი დაიკარგა ან მოიპარეს?

პასუხები აღნიშნულ და სხვა კითხვებზე განსხვავებული იქნება ორგანიზაციის მიხედვით, თუმცა, მნიშვნელოვანია ერთად ვიფიქროთ მათი საშუალებით და ნათლად განვაცხადოთ და გავაზიაროთ გეგმა ისე, რომ თქვენს ორგანიზაციაში ყველა მზად იყოს იმოქმედოს დაუყონებლივ ზიანის შეზღუდვის მიზნით. Tactical Tech-ის **„ყოვლისმომცველი უსაფრთხოების სახელმძღვანელოს“** თანახმად, ინციდენტზე რეაგირების გეგმის დასაწყებად კარგი პოზიციაა თქვენი ორგანიზაციის კონტექტში ინციდენტის ან ექტრემალური ვითარების განსაზღვრა. გადაწყვიტეთ რა არის „ექსტრემალური ვითარება“ – ანუ, მომენტი, რომელშიც უნდა დავიწყოთ დაგეგმილი ზომების მიღება და ანტიკრიზისული ღონისძიებების განხორციელება. ეს მნიშვნელოვანია, რადგან ხანდახან ის არ იქნება ნათელი – თუ წარმოიდგენთ სცენარს, როგორიცაა კავშირის დარღვევა სხვა კოლეგებთან საველე მისიისას; რამდენ ხანს დაელოდებით საგანგებო სიტუაციის გამოცხადებამდე? ზოგს არ სურს ზედმეტად ადრე დაწყება, თუმცა, ზედმეტად მოცდაც შესაძლოა დამღუპველი იყოს ზოგიერთ გარემოებაში.

ასევე მნიშვნელოვანია ბოლომდე გაიაზროთ ნებისმიერი **ოპერატიული** ნაბიჯებიც. დააკისრეთ თითოეულ პირს ნათელი როლის შესრულება, რომელზეც ის ინფორმირებულია და თანახმაა წინასწარ – აღნიშნული შეამცირებს დეზორგანიზაციას და პანიკას ინციდენტის შემთხვევაში. თითოეული საფრთხის შემთხვევაში გაითვალისწინეთ ის სხვადასხვა როლები, რომლებიც სასურველია, რომ იკისროთ ამ საგანგებო სიტუაციაზე რეაგირებისთვის. და საგანგებო სიტუაციაზე რეაგირების პრაქტიკული ასპექტები. საგანგებო სიტუაციების ხსენებული მნიშვნელოვანი სტრატეგიის ფარგლები მოიცავს მხარდამჭერი ქსელის აქტივაციას – მოკავშირეების ფართო ქსელი, რომელიც შესაძლოა მოიცავდეს მეგობრებს და ოჯახს, საზოგადოებას, ადგილობრივ მოკავშირეებს, სამთავრობო რესურსებს და მოკავშირეებს ეროვნულ თუ საერთაშორისო დონეზე, როგორიცა არასამთავრობო ორგანიზაციები და ჟურნალისტები. როგორ შეუძლიათ თქვენს მოკავშირეებს თქვენი მხარდაჭერა? უნდა დაუკავშირდეთ მათ წინასწარ იმის გადასამოწმებლად, რომ მათ ექნებათ სურვილი დაგეხმარონ საგანგებო სიტუაციაში და აცნობოთ მათ რას ელით მათგან?

საგანგებო სიტუაციაზე რეაგირებისას მზარდ მნიშვნელობას იძენს ეფექტური **კომუნიკაცია**. გადაწყვიტეთ თითოეულ მოქმედ პირთან კომუნიკაციის რომელი მაქსიმალურად დაცული და ეფექტური საშუალებები შედის სხვადასხვა სცენარში და მოახდინეთ სათადარიგო საშუალებების იდენტიფიკაცია. იცოდეთ, რომ საგანგებო სიტუაციებისათვის შესაძლოა სასარგებლო იყოს იქონიოთ ნათელი მითითებები მასზედ, თუ რა დაექვემდებაროს (და არ დაექვემდებაროს) კომუნიკაციას, როდის აწარმოოთ კომუნიკაცია, რომელი არხები გამოიყენოთ საკომუნიკაციოდ და ვისთან უნდა აწარმოოთ კომუნიკაცია. ასევე გაითვალისწინეთ საგანგებო სიტუაციის რეპუტაციული გავლენა თქვენს ორგანიზაციაზე და მზად იყავით შესაბამისად რეაგირებისათვიც. დარწმუნდით, რომ ორგანიზაციის კომუნიკაციის ხელმძღვანელობა (ზოგიერთ ორგანიზაციაში ეს შესაძლოა იყოს უბრალოდ ის, ვინც მართავს გვერდს Facebook-ში ან პროფილს Twitter-ში) ინფორმირებულია საგანგებო სიტუაციის შესახებ და შეუძლია თვალყური ადევნოს პოტენციურ გავლენას სოციალურ მედიაში და სხვა მედიაში. ისინი ასევე მზად უნდა იყვნენ, უპასუხონ საზოგადოების ან მედიის შესაძლო კითხვებს საგანგებო სიტუაციის შესახებ. ეს განსაკუთრებით მნიშვნელოვანია პოტენციური ნეგატიური ამბების ან რეპუტაციული ზიანის წინსწრებისათვის. მიუხედავად იმისა, რომ თითოეული საგანგებო სიტუაცია და კონტექსტი განსხვავებულია, გულწრფელი და გამჭვირვალე კომუნიკაცია ხშირად გეხმარებათ საგანგებო სიტუაციის შემდგომ ნდობის მოპოვებაში.



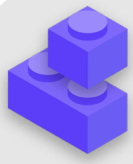
ადრეული განგაშის და რეაგირების სისტემის შექმნა

განიხილეთ ადრეული განგაშის და რეაგირების სისტემის ჩამოყალიბება. ხსენებული სისტემა უჩვეულოდ გამოიყურება, თუმცა, არსობრივად ესაა უბრალოდ ცენტრალიზებული დოკუმენტი (ელექტრონული ან სხვა ფორმით), რომელიც უნდა გაიხსნას საგანგებო სიტუაციაში. დოკუმენტში უნდა ჩაწეროთ უსაფრთხოების ინდიკატორების და იმ საგანგებო სიტუაციების ყველა დეტალი, რომლებსაც ადგილი აქვს დროთა განმავლობაში, ნათლად აღწეროთ ქმედებები და დაგეგმილი რეაგირების თანამიმდევრობა და აღნიშნოთ რა საჭიროებები უნდა იქნას მიღწეული იმის სათქმელად, რომ რისკი კიდევ ერთხელ შემცირდა. ის ასევე უნდა მოიცავდეს ქმედებებს, რომლებიც მიღებული უნდა იქნას საგანგებო სიტუაციის შემდეგ, რათა დაიცვათ მასში ჩართულები შემდგომი ზიანისაგან და დაეხმაროთ მათ ფიზიკურ და ემოციურ რეაბილიტაციაში. ადრეული განგაშის და რეაგირების სისტემამ შესაძლოა უზრუნველგყოთ სასარგებლო დოკუმენტაციით სამართალდამცველებთან (საჭიროების შემთხვევაში) გასაზიარებლად, მომხდარის შემდგომი ანალიზისათვის და იმის გასაგებად, თუ როგორ უნდა გაუმჯობესდეს თქვენი პრევენციის ტაქტიკა და საფრთხეებზე რეაგირება მომავალში.

გარდა საგანგებო სიტუაციაზე რეაგირების ხსენებული კონცეფციებისა, თქვენმა ორგანიზაციამ ასევე უნდა მოემზადოს ნებისმიერი სპეციფიური **ტექნიკური** რეაგირებისათვის. ზოგიერთ შემთხვევაში ტექნიკური რეაგირება შესაძლოა წარიმართოს It-ის საკუთარი პერსონალის ან სისტემური ადმინისტრატორების მიერ. მაგალითად, თუ ელ-ფოსტის პროფილი გატეხილი ჩანს, თქვენი პროფილის ადმინისტრატორი მზად უნდა იყოს და შეეძლოს გააუქმოს ან გამორთოს დაზარალებული პროფილი. თუმცა, ზოგიერთი ტექნიკური საგანგებო სიტუაცია შესაძლოა საჭიროებდეს ექსპერტულ ცოდნას, რომელიც არ გაგაჩნიათ თქვენი ორგანიზაციის ფარგლებში. მაგავს ვითარებაში, მნიშვნელოვანია გვქონდეს სანდო დამოუკიდებელი ტექნიკური ექსპერტების სია, ვისაც შეუძლიათ დაგეხმარონ საგანგებო სიტუაციაზე რეაგირებაში. ზოგიერთ შემთხვევაში, შესაძლოა გსურდეთ აწარმოოთ პირობებზე წინასწარი მოლაპარაკება სერვისის პროვაიდერებთან (როგორიცაა თქვენი ვებგვერდის ჰოსტი ან IT-ის საკითხებზე კონსულტანტი), რათა უზრუნველყოთ, რომ ისინი ხელმისაწვდომი არიან (და არ დაგაკისრებენ დამატებით ხარჯს) საგანგებო სიტუაციაზე ტექნიკური რეაგირებისათვის.

და ბოლოს, მაგრამ, რა თქმა უნდა, არა ბოლოში, უნდა დაფიქრდეთ **სამართლებრივ** ნაბიჯებზე. მნიშვნელოვანია თქვენი სამართლებრივი დაცვის შესაძლო საშუალებების, ასევე, სამართლებრივი ვალდებულებების და შედეგების გაგება, რომელთა წინაშეც შესაძლოა აღმოჩნდეს თქვენი ორგანიზაცია მონაცემების არასანქცირებული მიღების ან უსაფრთხოების სხვა ინციდენტის შედეგად. პირველი ნაბიჯი შესაძლოა იყოს სანდო ადვოკატების იდენტიფიკაცია, რომლებსაც ესმით თქვენი ქვეყნის თუ მდებარეობის კანონმდებლობა და რეგულაციები. საჭიროების შემთხვევაში, დაუთმეთ დრო შესაძლო საგანგებო სიტუაციების მიმოხილვას შესაბამის ადვოკატთან ერთად და შეადგინეთ გეგმა, თუ რას გააკეთებთ რეაგირების ფარგლებში. კარგი აზრია დადოთ ხელშეკრულება ხსენებულ სანდო ადვოკატთან, რომელიც წარმოგადგენთ თქვენ და თქვენს ინტერესებს საგანგებო სიტუაციის შემდგომ პერიოდში საჭიროების შემთხვევაში. როგორც აღნიშნული სამართლებრივი სამზადისის ნაწილი, დარწმუნდით, რომ გესმით ნებისმიერი მომწოდებლის თუ პარტნიორის სამართლებრივი ვალდებულებები. ვალდებულნი არიან ისინი, გაცნობონ მათი საკუთარი მონაცემების არასანქცირებული ხელყოფის თაობაზე? თქვენთვის რა მხარდაჭერის (ასეთის არსებობის შემთხვევაში) გაწევის მოვალეობა აქვთ მათ საგანგებო სიტუაციაში? დამოუკიდებელ მომწოდებლებთან კონტრაქტების და ხელშეკრულების შემუშავების შემდეგ გახსოვდეთ მონაცემთა არასანქცირებული ხელყოფის ან სხვა ინციდენტის შესაძლებლობის შესახებ.

რამდენადაც არ არსებობს საგანგებო სიტუაციებზე რეაგირებისადმი ერთგვაროვანი მიდგომა, მნიშვნელოვანია გქონდეთ ნათელი სამუშაო, საკომუნიკაციო, ტექნიკური და სამართლებრივი გეგმები. საგანგებო სიტუაციაზე რეაგირების გეგმის თქვენს მიერ კომპილაციის შემდეგ, დაბეჯითებით გირჩევთ გამოიყენოთ ზოგიერთი შესანიშნავი არსებული რესურსი, რომლის მიზანია დაეხმაროს სამოქალაქო საზოგადოებრივი ორგანიზაციებს და სხვა, მაღალი რისკის ჯგუფებს გაერკვიონ საგანგებო სიტუაციაზე რეაგირების საკითხებში. აღნიშნული რესურსები მოიცავს RaReNet-ის და CiviCERT-ის მიერ შემუშავებულ „პირველადი დახმარების ციფრულ კომპლექტს“, PEN America-ის „ონლაინ დევნის საველე სახელმძღვანელოს“, Belfer Center-ის „კიბერუსაფრთხოების კამპანიის სცენარებს“ და „კიბერ-ინციდენტების შეტყობინების მოდელ გეგმას“ და Access Now-ის „ციფრული უსაფრთხოების ცხელ ხაზს“.



რეაგირება საგანგებო სიტუაციაზე

- **შეიმუშავეთ განსაკუთრებულ შემთხვევებზე რეაგირების ორგანიზაციული გეგმა და მოახდინეთ მისი რეალიზაცია.**
  - კოლექტიურად იფიქრეთ შესაძლო საგანგებო სიტუაციებზე და მოემზადეთ რეაგირებისათვის მათ დადგომამდე.
- **უზრუნველყავით ორგანიზაციაში ყველას ინფორმირება, თუ როგორ აწარმოებთ კომუნიკაციას და რა ტექნიკური ნაბიჯები გადაიდგმება საგანგებო სიტუაციაში.**
- **დაუთმეთ დრო სამართლებრივი დაცვის თქვენი საშუალებების და ვალდებულებების შესწავლას.**
- **მზად იყავით გაუწიოთ ორგანიზაციის პერსონალს მისთვის საგანგებო სიტუაციის შემდეგ აუცილებელი ემოციური და სოციალური მხარდაჭერა.**

დანართი „ა“: რეკომენდებული რესურსები

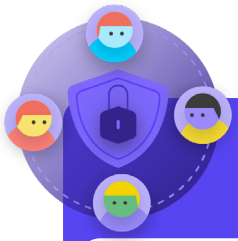
- Tactical Tech’s „თვალთვალისაგან თავდაცვის სახელმძღვანელო“; Creative Commons Attribution-ShareAlike 4.0 საერთაშორისო ლიცენზია
  - თავი 2.4 - ჩვენი ინფორმაციის გაგება და კატალოგიზება
  - თავი 1.5 - საფრთხეების შესახებ კომუნიკაცია გუნდებში და ორგანიზაციებში
  - თავი 3.4 - უსაფრთხოება ჯგუფებში და ორგანიზაციებში
- The Electronic Frontier Foundation’s Security Education Companion ; Creative Commons Attribution 3.0 US License
  - საფრთხის მოდელირების ღონისძიებების სამახსოვრო
- Freedom of the Press Foundation’s Phishing Prevention and Email Hygiene Guide; Creative Commons Attribution 4.0 International License
- Freedom of the Press Foundation-ის „გადაკეტვის სიგნალის სახელმძღვანელო“; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზია
- Electronic Frontier Foundation-ის „თვალთვალისაგან თავდაცვის (SSD) სახელმძღვანელო“; Creative Commons Attribution 3.0 აშშ-ის ლიცენზია
  - რა უნდა ვიცოდე დაშიფვრის შესახებ
  - სხვებთან კომუნიკაცია
  - თქვენთვის შესაფერისი VPN-ის არჩევა
- Frontline Defenders’ ის „უსაფრთხო ჯგუფური ჩეთის და საკონფერენციო ინსტრუმენტების სახელმძღვანელო“
- Tactical Tech’ ის „მონაცემთა დეტოქსიკაციის კომპლექტი“
  - შესაფერისის შერჩევა: გააძლიერეთ თქვენი პაროლები
  - გააუმჯობესეთ თქვენი ეკრანის ბლოკირება
- Center for Democracy and Technology-ის „არჩევნების უსაფრთხოების სახელმძღვანელო პაროლების შესახებ“; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზია
- Center for Democracy and Technology-ის „არჩევნების უსაფრთხოების სახელმძღვანელო აუთენტურობის ორფაქტორული შემოწმების შესახებ“; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზია
- Martin Shelton-ის „აუთენტურობის ორფაქტორული შემოწმება დამწყებთათვის“; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზია
- Tactical Tech and Frontline Defender-ის „უსაფრთხოება ყუთში“; Creative Commons Attribution-Share Alike 3.0 არაადაპტირებული ლიცენზია
  - დაიცავით თქვენი მოწყობილობა საზიანო პროგრამის და ფიშინგური შეტევებისაგან
  - დაიცავით თქვენი ინფორმაცია ფიზიკური საფრთხეებისაგან
- SANS-ის „ოჰ! ბიულეტენი: შეაჩერეთ ეს საზიანო პროგრამა
- Apple-ის „წვდომა მოწყობილობაზე და მონაცემებზე, როცა პირადი უსაფრთხოება საფრთხეშია“
- Global Cyber Alliance-ის „კიბერ-ჰიგიენა მისიის ტიპის ორგანიზაციებისათვის“

დანართი „ბ“: უსაფრთხოების გეგმის საწყისი კომპლექტი

გამოიყენეთ შემდეგი საწყისი კომპლექტი ჩანაწერების გასაკეთებლად თქვენი და თქვენი ორგანიზაციის მიერ „სახელმძღვანელოს“ გაცნობისას და მასალის გაცნობიერებისას და განიხილეთ თანმდევი კითხვები თქვენს კოლეგებთან, რათა წარმოებული იქნას პროდუქტიული დისკუსია.

აუცილებლად მიუთითეთ საკვანძო შემადგენელი ბლოკები სახელმძღვანელოს თითოეულ სექციაში, რათა დარწმუნდეთ, რომ ეხებით მნიშვნელოვან თემებს უსაფრთხოების საკუთარი გეგმის შედგენისას. სახელმძღვანელოს ბოლოს, შემადგენელმა ბლოკებმა, ამ სადისკუსიო კითხვებზე პასუხებმა და თქვენმა ჩანაწერებმა უნდა შეადგინოს უსაფრთხოების წარმატებული გეგმის საფუძველი!





უსაფრთხოების კულტურის დანერგვა

განსახილველი კითხვები:

- როდის შეგიძლიათ დაგეგმოთ საუბარი მთელს ორგანიზაციასთან უსაფრთხოების თქვენი გეგმის განსახილველად?
- რომელი დღეები ან დროა მისაღები ორგანიზაციისათვის რეგულარული საუბრების და უსაფრთხოების საკითხებზე ტრენინგის დასაგეგმად?
- რა ზომების მიღება შეუძლია ხელმძღვანელობას უსაფრთხოების სწორი ქცევის და უსაფრთხოების გეგმის მიმართ პასუხისმგებლობის მოდელის შესაქმნელად? როგორ შეუძლიათ ორგანიზაციის სხვა თანამშრომლებს, შეიტანონ წვლილი უსაფრთხოებაში?

თქვენი ჩანაწერები და იდეები:



მყარი საფუძველი: პროფილების და მოწყობილობების დაცვა

განსახილველი კითხვები:

- როგორ განახორციელებთ პროფილის უსაფრთხოების ღონისძიებებს - როგორიცაა პაროლების დისპეტჩერი და and 2FA-ი - მთელს ორგანიზაციაში? რა სირთულეებს შესაძლოა გადააწყდეთ განხორციელების პროცესში?
- როგორ უზრუნველყოფს თქვენი ორგანიზაცია, რომ მოწყობილობები იყოს დაცული და განახლებული? როგორც აღნიშნულის ნაწილი, დასჭირდება ორგანიზაციას გეგმა არალიცენზირებული პროგრამული უზრუნველყოფის თუ კომპიუტერების საკითხის მოსაგვარებლად?
- როდისაა დროული გამართოთ ტრენინგი მთელი პერსონალისათვის ფიშინგის და საზიანო პროგრამის საფრთხეების და მოწყობილობის უსაფრთხოების აღიარებული პრაქტიკის თაობაზე?

თქვენი ჩანაწერები და იდეები:

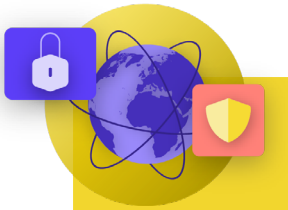


უსაფრთხო კომუნიკაცია და მონაცემების შენახვა

განსახილველი კითხვები:

- როგორ განახორციელებს თქვენი ორგანიზაცია აბონენტური დაშიფვრით შეტყობინებების მიმოცვლას დაცული კომუნიკაციისათვის? რა სირთულეებს შესაძლოა გადააწყდეთ განხორციელების პროცესში?
- როგორ აღასრულებს თქვენი ორგანიზაცია ფაილების დაცული გაზიარების გადაწყვეტას როგორც შიგნით, ისე გარეთ? რა სირთულეებს შესაძლოა გადააწყდეთ განხორციელების პროცესში?
- როგორ განახორციელებს თქვენი ორგანიზაცია მონაცემთა დაცული შენახვის და რეზერვის შექმნის გადაწყვეტას? რა სირთულეებს შესაძლოა გადააწყდეთ განხორციელების პროცესში?

თქვენი ჩანაწერები და იდეები:



უსაფრთხოების დაცვა ინტერნეტში

განსახილველი კითხვები:

- როგორ განახორციელებს თქვენი ორგანიზაცია პერსონალისათვის უსაფრთხო ბრაუზინგის მოთხოვნებს, როგორიცაა HTTPS-ი, სანდო ბრაუზერი და, შესაბამისობის შემთხვევაში, VPN-ი?
- რა იქნება თქვენი ორგანიზაციის სოციალური მედიის პოლიტიკის საკვანძო ელემენტები? როგორ აღსრულდება ის?
- როგორ დაიცავს თქვენი ორგანიზაცია საკუთარ ვებგვერდებს და ვებ-რესურსებს?

თქვენი ჩანაწერები და იდეები:



ფიზიკური უსაფრთხოების დაცვა

განსახილველი კითხვები:

- როგორ გაავრცელებს და აღასრულებს ორგანიზაცია ოფისის სტუმრების და წვდომის საკუთარ პოლიტიკას?
- ვინ არის პასუხისმგებელი პერსონალის მომზადებაზე ფიზიკური და ციფრული უსაფრთხოების იმ გამოწვევებზე, რომელთა წინაშეც ისინი შესაძლოა აღმოჩდნენ მოგზაურობის ან მუშაობისას?
- რა ნაბიჯების გადადგემა შეუძლია პერსონალს საკუთარი მოწყობილობების დასაცავად და უსაფრთხოებისათვის როგორც ოფისში, ისე მოგზაურობისას?

თქვენი ჩანაწერები და იდეები:



როგორ იქცევით, როცა საქმე ცუდადაა

განსახილველი კითხვები:

- როგორ აწარმოებს ორგანიზაცია საგანგებო საგანგებო სიტუაციაზე რეაგირების გეგმის გავრცელებას და რეალიზაციას?
- არსებობს იმ პერსონალისათვის ხელმისაწვდომი რესურსები, რომელსაც შესაძლოა დასჭირდეს ემოციური და სოციალური მხარდაჭერა საგანგებო სიტუაციის შემდეგ? თუ არა, როგორ შეიძლება ორგანიზაციამ უზრუნველყოს ხსენებული რესურსები საგანგებო სიტუაციაში?

თქვენი ჩანაწერები და იდეები:

დანართი „გ“: გამოსახულებით ციტირება

გვერდი 17: CNP Collection, „Security Protection Anti-Virus Software cms"-ი, 2014 წ., ციფრული გამოსახულება, Alamy Stock Photo-ი, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_

source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.

გვერდი 24: Cottonbro-ი, „Person Holding Black and Silver Key"-ი, 2020 წ., ციფრული გამოსახულება, Pexels-ი, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

გვერდი 26: Blogtrepreneur-ი, „Malware Infection"-ი, 2016 წ., ციფრული გამოსახულება, Flickr-ი, https://www.flickr.com/photos/143601516@N03/.

გვერდი 29: „Microsoft Loading Screen"-ი, ციფრული გამოსახულება, Kompass-ი, 2019 წ. 23 სექტემბერი, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.

გვერდი 30: Mateuz Dach-ი, „Turned-on iPhone and Displaying Icons"-ი, 2017 წ., ციფრული გამოსახულება, Pexels-ი, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

გვერდი 33: Crete-Nishihata-ი, „Process For a Phishing Email Sent in 2016“-ი, ციფრული გამოსახულება, ტორონტოს უნივერსიტეტი, 2017 წ, 30 იანვარი, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/.

გვერდი 38: Andrew Keymaster-ი, „People Gathering on Street During Daytime Photo"-ი, 2020 წ., ციფრული გამოსახულება, Unsplash-ი, https://unsplash.com/photos/JXQ2bizu7kc.

გვერდი 39: Surveillance Self-Defenseი, „No Encryption in Transit"-ი, ციფრული გამოსახულება, Electronic Frontier Foundation-ი, 2019 წ. 17 იანვარი.
https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

გვერდი 40: Surveillance Self-Defense-ი, „4.Transport-layer-alternate"-ი, ციფრული გამოსახულება, Electronic Frontier Foundation-ი, 2019 წ. 17 იანვარი, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense-ი, „6. End-to-end Alternate"-ი, ციფრული გამოსახულება, Electronic Frontier Foundation-ი, 2019 წ. 17 იანვარი, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.

გვერდი 42: Surveillance Self-Defense-ი, „9._endtoendencryptionmetadata"-ი, 2019 წ., ციფრული გამოსახულება, Electronic Frontier Foundation-ი, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

გვერდი 50: Brett Sayles-ი, „Server Racks on Data Center"-ი, 2020 წ., ციფრული გამოსახულება, Pexels-ი, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

გვერდი 55: PhotoMIX Company-ი, 2016 წ., „White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky"-ი, ციფრული გამოსახულება, Pexels-ი, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.

გვერდი 60: Stefan Coders-ი, „laptop-screen-vpn-cyber-security"-ი, 2020 წ., ციფრული გამოსახულება, Unsplash-ი, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

გვერდი 62: Surveillance Self-Defense-ი, „Using the Tor Browser"-ი, ციფრული გამოსახულება, Electronic Frontier Foundation-ი, 2020 წ. 25აპრილი. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

გვერდი 64: Nathan Dumlao-ი, „White Samsung Android Smartphone on Brown Wooden Table"-ი, 2020 წ., ციფრული გამოსახულება, Unsplash-ი, https://unsplash.com/photos/kLmt1mpGJVg.

გვერდი 69: Matt Artz-ი, „Two Broken 6-Pane On White Painted Wall Photo"-ი, ციფრული გამოსახულება, Unsplash-ი, 2017 წ. 1 ოქტომბერი, https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE

