NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

კიბერუსაფრთხოების სახელმძღვანელო

თქვენი

პარლამენტებისთვის

სახელმძღვანელო პარლამენტებისთვის, რომლებიც გეგმავენ კიბერუსაფრთხოების გეგმაზე გადასვლას

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID FROM THE AMERICAN PEOPLE

NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP
UNITED STATES HOUSE OF REPRESENTATIVES

კიბერუსაფრთხოების სახელმძღვანელო

თქვენი

პარლამენტებისთვის

სახელმძღვანელო პარლამენტებისთვის, რომლებიც გეგმავენ კიბერუსაფრთხოების გეგმაზე გადასვლას

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

შინაარსი

ვიზუალური აღნიშნვები

სახელმძღვანელოში, ძირითადი ტექსტის გარდა, შეგხვდებათ რამდენიმე განსხვავებული განმეორებადი, გამოკვეთილი ელემენტი. აქ არის მოკლე „აღნიშვნა“, რომელიც დაგეხმარებათ ძირითადი ელემენტების გაგებაში:

შემთხვევის ანალიზი

მოიცავს შემთხვევების ანალიზს, სადაც ხაზგასმულია გარკვეული თემის რეალური გავლენა პარლამენტებზე გლობალურად ან კონკრეტულ ქვეყანაში.

დამატებითი რჩევები

გამოყოფს დამატებით რეკომენდაციებს და ინფორმაციას, რომელიც საყურადღებოა სახელმძღვანელოს კითხვის დროს.

რეალური სამყარო

მოჰყავს კიბერუსაფრთხოების ინსტრუმენტების ზოგადი მაგალითები, როგორც კარგი, ასევე ცუდი, რომელსაც შეხვდებით „რეალურ სამყაროში“.

ღრმად

მიუთითებს გაფართოებულ თემაზე - ინფორმაციაზე, რომელიც პარლამენტისთვის მნიშვნელოვანია გასათვალისწინებლად, მაგრამ შეიძლება იყოს უფრო ტექნიკური ან რთული გასაგები.

უსაფრთხოების გეგმის შემადგენელი ბლოკები

მიუთითებს „უსაფრთხოების გეგმის შემადგენელ ბლოკებზე“, რომლებიც სახელმძღვანელოს თითოეული სექციიდან ძირითად ასათვისებელ მასალას წარმოადგენს.

ტოპ 10

ეს 10 ელემენტი პარლამენტის უსაფრთხოების გეგმისთვის კრიტიკულად მნიშვნელოვანია. თუ გსურთ საიდანმე დაწყება, ჯერ დაიწყეთ აქედან.

1. ჩაატარეთ რეგულარული უსაფრთხოების ტრენინგი პარლამენტში
2. უფრთხილდით ფიშინგს და გქონდეთ გამართლი აანგარიშგების სისტემა
3. ყველა კომუნიკაციისთვის გამოიყენეთ შიფრაცია - თავიდან ბოლომდე, სადაც ეს შესაძლებელია
4. მოითხოვეთ ძლიერი პაროლები და პარლამენტში დანერგეთ პაროლის მენეჯერი
5. მოითხოვეთ ორფაქტორიანი ავთენტიფიკაცია, სადაც ეს შესაძლებელია
6. დარწმუნდით, რომ პერსონალის ყველა მოწყობილობა და პროგრამული უზრუნველყოფა განახლებულია
7. გამოიყენეთ დაცული დისტანციური საცავი მონაცემთა შესანახად
8. ინტერნეტზე წვდომისთვის გამოიყენეთ HTTPS და, საჭიროების შემთხვევაში, VPN
9. დაიცავით თქვენი პარლამენტის ფიზიკური აქტივები
10. შეიმუშავეთ ორგანიზაციაში ინციდენტზე რეაგირების გეგმა

1

უსაფრთხოების კულტურის დანერგვა

2

მყარი საფუძველი: ანგარიშებისა და მოწყობილობების დაცვა

3

უსაფრთხო კომუნიკაცია და მონაცემების უსაფრთხოდ შენახვა

4

უსაფრთხოების დაცვა ინტერნეტში

5

ფიზიკური უსაფრთხოების დაცვა

6

როგორ იქცევით როცა საქმე ცუდადაა

ავტორები და აღიარება

ეს სახელმძღვანელო მომზადებულია ეროვნულ-დემოკრატიული ინსტიტუტის (NDI) და დემოკრატიული პარტნიორობის პალატის (HDP) მიერ.

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 და 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; Aaron Azelton, NDI; Frieda Arenos, NDI; Anthony DeAngelo, NDI; Whitney Pfeifer, NDI; და Derek Luyten, House Democracy Partnership ასევე გვინდა მადლობა გადავუხადოთ ლიბერიის საკანონმდებლო საინფორმაციო სამსახურის თანამშრომელს Paul Kollie, Nihad Bahram და Fuad Ahmed ერაყის ქურთისტანის პარლამენტიდან, Diana Plata-ს კოლუმბიის სენატიდან; Ayad Abbas და Majid Khudhur ერაყის წარმომადგენელთა საბჭოსა და Tanja Danailovska-ს ჩრდილოეთ მაკედონიის ასამბლეიდან მათი ღირებული იდეებისა და წვლილისთვის.

ასევე გვსურს, აღვნიშნოთ ორგანიზაციული უსაფრთხოების საზოგადოების (OrgSec) მიერ შედგენილი ყველა შესანიშნავი სახელმძღვანელო, ცნობარი, დამხმარე სახელმძღვანელო, ტრენინგის მოდული და სხვა მასალა. მოცემული სახელმძღვანელო მიზნად ისახავს თავი მოუყაროს უფრო დეტალურ ინფორმაციას საკვანძო გაკვეთილების გაერთიანების გზით, ერთსაფეხურიან, ადვილად წასაკითხ მასალაში პარლამენტებისთვის, რომლებსაც სურთ გადავიდნენ კიბერუსაფრთხოების გეგმაზე.

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 იხ. ხსენებული რესურსების სპეციფიური ციტირებები, ხოლო რესურსების გვერდზე მოცემულია სრულ ბმულები, ავტორი და სალიცენზიო ინფორმაცია. ქვემოთ მოცემულ სექციებში მრავლად შეხვდებით ხსენებული რესურსების სპეციფიურ ციტირებებს, ხოლო დანართში „ა“ მოცემულია სრულ ბმულები, ავტორი და სალიცენზიო ინფორმაცია.

ვინ ვართ ჩვენ?

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. თქვენ შეგიძლიათ გაიგოთ მეტი ჩვენი მუშაობის შესახებ ვებგვერდიდან website, გამოგვყევით Twitter-ზე, ან პირდაპირ დაგვიკავშირდით მისამართზე cyberhandbook@ndi.org. ყოველთვის მოხარულნი ვართ, მივიღოთ თქვენი გამოხმაურება და ვუპასუხოთ შეკითხვებს, რომლებიც ეხება ჩვენს გუნდს და საქმიანობას კიბერუსაფრთხოების, ტექნოლოგიებისა და დემოკრატიის მხრივ.

პალატის დემოკრატიული პარტნიორობა (HDP) თანამშრომლობს საკანონმდებლო ორგანოებთან მთელს მსოფლიოში, რათა ხელი შეუწყოს პასუხისმგებელ, ეფექტურ მმართველობას და გააძლიეროს დემოკრატიული ინსტიტუტები. ჩვენს საქმიანობაში მთავარია პარტნიორებთან თანამშრომლობა, რათა პარტნიორ საკანონმდებლო ორგანოებში შეიქმნას ტენიკური საფუძველი, რაც გაზრდის ანგარიშვალდებულებას, გამჭვირვალობას, საკანონმდებლო ორგანოს დამოუკიდებლობას, ინფორმაციის ხელმისაწვდომობას და მთავრობის ზედამხედველობას. HDP ამჟამად 20-ზე მეტ ეროვნულ საკანონმდებლო ორგანოსთან თანამშრომლობს მთელს მსოფლიოში. HDP-ის პარტნიორ პარლამენტებთან თანამშრომლობის სფეროები მოიცავს საბიუჯეტო საკითხების მოგვარებას, კომიტეტების მუშაობის ეფექტურობის გაზრდას, ამომრჩეველთა მომსახურების გაუმჯობესებას, უფრო ძლიერი ზედამხედველობის ინსტრუმენტებით უზრუნველყოფას, საკანონმდებლო ეთიკის გაძლიერებას და საინფორმაციო ტექნოლოგიების, ბიბლიოთეკებისა და კვლევით სერვისების საკანონმდებლო პროცესებისა და პროცედურების გაუმჯობესებას. HDP-ის პროგრამები ხორციელდება ეროვნული დემოკრატიული ინსტიტუტი (NDI) და საერთაშორისო რესპუბლიკური ინსტიტუტი (IRI) დახმარებით აშშ-თან თანადაფინანსების ხელშეკრულების საფუძველზე. საერთაშორისო განვითარების სააგენტო (USAID).

ვინ მართავს საპარლამენტო კიბერუსაფრთხოებას?

ეფექტური და უსაფრთხო პარლამენტი საჭიროებს პერსონალს, რომელსაც აქვს უნარები და შესაფერისი უფლებამოსილება, რომ განახორციელოს წინამდებარე სახელმძღვანელოში მოცემული რეკომენდაციები. აღნიშნულიდან გამომდინარე, პარლამენტებში კიბერუსაფრთხოებაზე პასუხისმგებელი პირები შეიძლება ძალიან განსხვავდებოდეს და არ არსებობს კონკრეტული „სწორი“ მოდელი, თუ ვინ უნდა იყოს კიბერუსაფრთხოებაზე პასუხისმგებელი. ზოგიერთ შემთხვევაში, ეს შეიძლება იყოს კიბერუსაფრთხოების სპეციალური გუნდი IT დეპარტამენტში, ზოგჯერ კი ეს შეიძლება იყოს სხვადასხვა ადმინისტრაციული პერსონალი და თანამშრომლები. გაითვალისწინეთ, მიუხედავად იმისა, რომ მნიშვნელოვანია გყავდეთ პარლამენტის კიბერუსაფრთხოებაზე პასუხისმგებელი კარგი გუნდი, ყველას პასუხისმგებლობაა, პარლამენტში და მის გარშემო დაიცვას პარლამენტის უსაფრთხოებისთვის აუცილებელი პოლიტიკა და პროცედურები. ქვემოთ მოცემულია საპარლამენტო კიბერუსაფრთხოების მართვის სხვადასხვა პერსონალის მოდელების რამდენიმე მაგალითი:

აშშ-ს წარმომადგენელთა პალატა
საინტერესოა, რომ **აშშ-ის წარმომადგენელთა პალატა**-ში, ზოგიერთი ოფისი ქირაობს **სისტემური ადმინისტრატორი**, რომელიც პასუხისმგებელია ოფისის მიერ გამოყენებული ყველა კომპიუტერული ტექნიკისა და პროგრამული სისტემის მართვაზე, მათ შორის კიბერუსაფრთხოების საკითხების მართვაზე - და თანამშრომლების მომზადების მოწინავე მეთოდებზე. ინსტიტუციურ დონეზე, წარმომადგენელთა პალატის მთავარ ადმინისტრაციულ ოფიცერს შემადმგენლობაში ჰყავს საინფორმაციო რესურსების ჯგუფი, რომელიც მოიცავს **ინფორმაციულ უსაფრთხოებასთან დაკავშირებულ დეპარტამენტს.**

ზამბიის ეროვნული ასამბლეა
ზამბიის ეროვნული ასამბლეა-ს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების დეპარტამენტის (ICT) იმედი აქვს სხვადასხვა ფუნქციების შესასრულებლად, მათ შორის პარლამენტის პროგრამული უზრუნველყოფის, აპარატურის და საინფორმაციო ინფრასტრუქტურის მართვის, წევრების ტრენინგის ან პარლამენტის და პერსონალის ტექნოლოგიების შერჩევის შემთხვევაში, სისტემების და პარლამენტის საინფორმაციო ინფრასტრუქტურის შიდა და გარე კიბერ საფრთხეებისგან დაცვაში.

მალაიზიის პარლამენტი
მალაიზიის **დპარლამენტში** არის საინფორმაციო ტექნოლოგიების დეპარტამენტი, რომელიც ექვემდებარება პარლამენტის მთავარ ადმინისტრატორს, რაც საშუალებას აძლევს მას მოემსახუროს პარლამენტის ორივე პალატას. ამ ერთეულს აქვს ქსელის უსაფრთხოების კონრეტული პოზიცია, რაც საშუალებას აძლევს მას უზრუნველყოს ქსელური სისტემების, მონაცემთა ცენტრების და ICT ინფრასტრუქტურის შესაბამისობა და მაქსიმალური უსაფრთხოება.

ვისთვისაა გამიზნული წინამდებარე „სახელმძღვანელო“?

წინამდებარე „სახელმძღვანელო“ დაიწერა მარტივი მიზნით: დახმარებოდა პარლამენტს კიბერუსაფრთხოების გასაგები და რეალიზებადი გეგმის შემუშავებაში.

რამდენადაც სამყარო სულ უფრო და უფრო გადადის ონლაინ რეჟიმზე, კიბერუსაფრთხოება უკვე აღარ არის მხოლოდ მოდური სიტყვა, არამედ პარლამენტების წარმატებისთვის საჭირო კრიტიკული კონცეფცია და ინფორმაციის უსაფრთხოება (როგორც ონლაინ, ისე ოფლაინ) არის გამოწვევა, რომელიც მოითხოვს ყურადღებას, ინვესტიციებს და სიფხიზლეს.

თქვენი პარლამენტი სავარაუდოდ - თუ უკვე არა - იქნება კიბერშეტევის სამიზნე. ეს არაა პანიკიორობა; ეს რეალობაა იმ პარლამენტებისთვისაც კი, რომლებიც არ მიიჩნევენ 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 წარმოადგენს სამიზნეს ერთბაშად, ასეულობით თუ არა, ათეულობით ორგანიზაციას მაინც. ამ ინფორმირებული შეტევების გარდა, არის ალბათ ასობით სხვა უფრო მცირე შეტევა, რომლებიც ყოველწლიურად შეუმჩნეველია ან არ ხდება მათი შეტყობინება, რომელთაგან ბევრის სამიზნეს წარმოადგენს სამთავრობო უწყებები, საკანონმდებლო ორგანოები და პოლიტიკური ორგანიზაციები.

აღნიშნულის მსგავს კიბერ-შეტევებს გააჩნია მნიშვნელოვანი შედეგები. მათ მიზანს წარმოადგენს პარლამენტის საქმიანობის ჩაშლა, რეპუტაციის შელახვა ან თუნდაც ინფორმაციის მოპარვა, რამაც შეიძლება ფსიქოლოგიური ან ფიზიკური ზიანი მიაყენოს პარლამენტის წევრებს ან თანამშრომლებს, მაგალითად მუქარა, სერიოზულად უნდა იქნას აღქმული.

კარგი ისაა, რომ თქვენი და თქვენი პარლამენტის საყოველთაო საფრთხეებისაგან დასაცავად არაა საჭირო იქცეთ პროგრამისტად ან ტექნოლოგად. თუმცა, მყარი საპარლამენტი უსაფრთხოების გეგმის შემუშავების და რეალიზაციისას მზად უნდა იყოთ ძალისხმევის, ენერგიის და დროის ინვესტიციისთვის.

თუ არასოდეს გიფიქრიათ პარლამენტის კიბერუსაფრთხოებაზე, ამაზე ფოკუსირებისთვის არ გქონდათ დრო, ან იცნობთ თემის ზოგიერთ საფუძველს, მაგრამ ფიქრობთ, რომ თქვენს პარლამენტს შეუძლია გააუმჯობესოს კიბერუსაფრთხოება, ეს სახელმძღვანელო თქვენთვისაა. **მიუხედავად იმისა, თუ საიდან ხართ, ეს სახელმძღვანელო შექმნილია იმისთვის, რომ თქვენს პარლამენტს მიაწოდოს ის ინფორმაცია, რომელიც მას სჭირდება ძლიერი უსაფრთხოების გეგმის შესამუშავებლად - გეგმა, რომელიც სცილდება მხოლოდ სიტყვების ქაღალდზე დაწერას და საშუალებას გაძლევთ დანერგოთ საუკეთესო პრაქტიკა.**

რა არის უსაფრთხოების გეგმა და რატომ უნდა ჰქონდეს ის პარლამენტს?

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 პარლამენტის 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 პარლამენტს, აღიქვას თქვენ 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 პარლამენტს ხსენებული პროცესის გავლაში. თუ თქვენ გაქვთ ამ დონის პროფესიონალური გამოცდილება, ეს ამად ღირს, მაგრამ მაშინაც კი, თუ ვერ გაივლით სრულ შეფასებას, უნდა შეხვდეთ დაინტერესებულ მხარეებს პარლამენტში, რათა განიხილოთ შემდეგი ძირითადი საკითხები:

1 რა აქტივები აქვს თქვენს პარლამენტს და რისი დაცვა გსურთ?

თქვენ შეგიძლიათ დაიწყოთ ამ კითხვებზე პასუხის გაცემა **თქვენი პარლამენტის მთელი აქტივების 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 პარლამენტის 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 ჩვეულებრივ 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 მაგალითებია ფინანსური თაღლითები, მტრულად განწყობილი მთავრობები ან იდეოლოგიურად ან პოლიტიკურად მოტივირებული ჰაკერები. მნიშვნელოვანია, შეადგინოთ თქვენი მეტოქეების სია და კრიტიკულად შეაფასოთ ვის შეიძლება სურდეს თქვენს პარლამენტზე 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. ისინი დაინტერესებულნი არიან თქვენი პარლამენტის დისკრედიტაციით? იქნებ თქვენი გზავნილის მიჩუმებას ან პარლამენტის ჩაშლას აპირებენ? მნიშვნელოვანია, გავიგოთ მეტოქის მოტივაცია, რადგან ეს შეიძლება დაეხმაროს თქვენს პარლამენტს, უკეთ შეაფასოს საფრთხეები, რომლებიც მან შეიძლება წარმოქმნას.

3 რა საფრთხეების წინაშე დგას თქვენი პარლამენტი? და რამდენად რეალური და გავლენიანია ისინი?

შესაძლო საფრთხეების იდენტიფიკაციის შემდეგ, სავარაუდოდ, გექნებათ გრძელი სია, რომელიც შეიძლება გადაჭარბებული აღმოჩნდეს. შესაძლოა, იგრძნოთ, რომ ნებისმიერი ძალისხმევა უსაგნოა ან არ იცოდეთ, საიდან დაიწყოთ. თქვენი პარლამენტის 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.

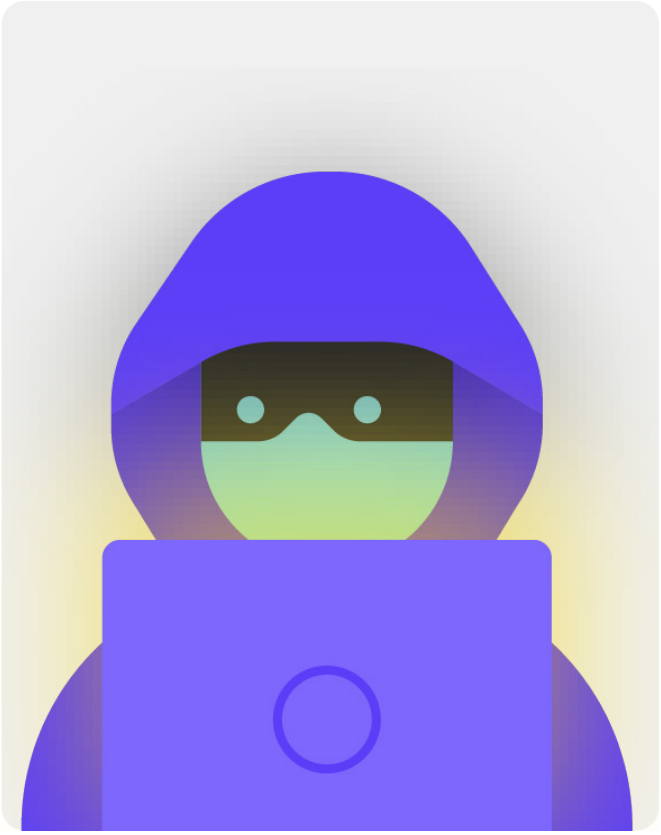
საფრთხის ალბათობის გასაზომად (სავარაუდოდ „დაბალი, საშუალო ან მაღალი“ იმის და მიხედვით, რომ მოცემული შემთხვევა ნაკლებად სავარაუდოა, მოხდეს, შესაძლოა, მოხდეს ან ხდება ხშირად), შეგიძლიათ, გამოიყენოთ მეტოქეების შესაძლებლობებზე თქვენთვის ცნობილი ინფორმაცია, უსაფრთხოების წარსული ინციდენტების ანალიზი, სხვა მსგავსი პარლამენტის გამოცდილება და, რა თქმა უნდა, თქვენი პარლამენტის 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 პარლამენტი და როგორც ხალხი, ფიზიკურად და მენტალურად?“, „რამდენად გრძელვადიანი იყო ეფექტი?“, „წარმოშობს ეს სხვა საზიანო სიტუაციებს?“ და „რამდენად ამცირებს ის ჩვენს უნარს, მივაღწიოთ ჩვენს 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 კარგია: ბევრი რამის გაკეთება შეგიძლიათ საკუთარი თავის, კოლეგების და პარლამენტის დასაცავად ყველაზე სერიოზულ საფრთხეებზე ფოკუსირების გზით.

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 პარლამენტისთვის კიბერუსაფრთხოების გეგმის შექმნა

მიუხედავად იმისა, რომ პარლამენტის უსაფრთხოების გეგმა მცირედ განსხვავებულად გამოიყურება გამომდინარე მისი რისკების შეფასებიდან და ორგანიზაციული დინამიკიდან, ზოგიერთი საკვანძო კონცეფცია თითქმის უნივერსალურია.

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

წინამდებარე „სახელმძღვანელო“ უზრუნველყოფს შეთავაზებებს და ოფციებს, რომლებიც უფასო ან მეტად იაფია. გაითვალისწინეთ, რომ ყველაზე მნიშვნელოვანი ფასეულობა, რომელიც დაკავშირებულია უსაფრთხოების ეფექტური გეგმის განხორციელებასთან, იქნება დრო, რომელიც დაგჭირდებათ თქვენ და თქვენს თანამშრომლებს, წევრებს და გუნდებს თქვენი ახალი გეგმის შესწავლის, განხილვისა და განხორციელებისთვის. იმის გათვალისწინებით, თუ რა რისკებს შეიძლება დაუპირისპირდეს პარლამენტი, ეს ინვესტიცია კიდევ უფრო ღირებულია.

თითოეულ სექციაში შეგხვდებათ იმ საკვანძო საკითხის განმარტება, რომლის თაობაზეც ინფორმირებული უნდა იყოს თქვენი პარლამენტი 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 პარლამენტში.

უსაფრთხოების გეგმის საწყისი კომპლექტი

თქვენი პარლამენტის 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. როდესაც დაიწყებთ შენიშვნების ჩაწერას და განახლებას, ან ახალი უსაფრთხოების გეგმის შექმნას, ისარგებლეთ „უსაფრთხოების გეგმის შემადგენელი ბლოკებით“, რომელიც დეტალურად არის გაწერილი თითოეულ სექციაში. უსაფრთხოების გეგმა ვერ იქნება სრული მინიმუმ ხსენებული არსებითი ელემენტების მითითების გარეშე.

გამოიყენეთ სხვა რესურსები, რომლებიც ასევე შეიძლება დაგეხმაროთ თქვენი გეგმის შედგენაში და რეალიზაციაში.
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

უსაფრთხოება უშალოდ ადამიანებს ეხება და პარლამენტის დასაცავად, თქვენ უნდა დარწმუნდეთ, რომ ყველა ჩართულია პროცესში - მათ შორის პარლამენტის წევრები, საკანონმდებლო მხარდაჭერისა და კვლევის ოფიცრები და ფინანსების, ადამიანური რესურსების და IT ადმინისტრაციული ოფიცრები და მრავალი სხვა - და სერიოზულად ეკიდება კიბერუსაფრთხოებას. კულტურის შეცვლა რთულია, თუმცა, რამდენიმე მარტივმა ნაბიჯმა და მნიშვნელოვანმა საუბარმა შეიძლება მყისიერად მიგიყვანოთ ატმოსფერომდე, რომელიც აამოქმედებს თქვენი პერსონალის და პარლამენტის კიბერუსაფრთხოების მოქნილ სტრატეგიას უსაფრთხოების წინაშე არსებული საფრთხეების პასუხად. ერთ-ერთი უმარტივესი, მაგრამ ყველაზე მნიშვნელოვანი ნაბიჯი, რომელიც უნდა გადაიდგას ამ საპარლამენტო უსაფრთხოების კულტურის შესაქმნელად, არის მის შესახებ კომუნიკაცია პარლამენტში და ლიდერებმა ყოველთვის უნდა მიმართონ კარგი ქცევის მოდელს და გააკეთონ მასში ინვესტიცია.

უსაფრთხოების კულტურის ჩამოყალიბება პარლამენტებში

2019 წლის თებერვალში ავსტრალიამ განიცადა კიბერშეტევა, რა დროსაც მოხდა ავსტრალიის ეროვნული პარლამენტისა და სამი წამყვანი პოლიტიკური პარტიის ქსელში შეღწევა. თავდამსხმელებმა მოიპოვეს პოლიტიკურ დოკუმენტებზე და პარლამენტარებს შორის, მათ თანამშრომლებსა და ამომრჩევლებს შორის ელექტრონულ მიმოწერაზე წვდომა. თავდასხმა დაგეგმილ არჩევნებამდე სამი თვით ადრე მოხდა, რამაც ხაზი გაუსვა არჩევნების დროს ქსელების დაუცველობას.

ამ დიდი და წარმატებული თავდასხმის საპასუხოდ, პარლამენტმა გაზარდა კიბერუსაფრთხოებისთვის მზაობა. ასეთი ინვესტიციები მოიცავდა საჯარო ანგარიშების ერთობლივი კომიტეტისა და თანამეგობრობის კიბერგამძლეობის აუდიტის მიერ ჩატარებულ გამოძიებას. გამოძიებამ [აუდიტის შედეგებზე დაყრდნობით](), რომელიც მიმდინარეობდა რამდენიმე წლის განმავლობაში, გამოავლინა კიბერუსაფრთხოების რისკის შემცირების პროცესების ნაკლებობა პარლამენტში და სხვა საჯარო დაწესებულებებში. მაგალითად, ავსტრალიის ეროვნულმა აუდიტის ოფისმა ხაზი გაუსვა პარლამენტის პრობლემას, რომ მან ფოკუსირება უნდა მოახდინოს გრძელვადიან სტრატეგიულ მიზნებზე და განავითაროს კიბერუსაფრთხოების რისკზე დაფუძნებული მიდგომა. მიუხედავად იმისა, რომ გამოძიებები და მიმოხილვები არ მიმდინარეობდა სასიამოვნოდ, პარლამენტის მზადყოფნა იდენტიფიცირება და ინვესტირება მოეხდინა კიბერუსაფრთხოების საკითხებში, არის ეფექტური საპარლამენტო კიბერუსაფრთხოების კულტურის დანერგვის მაგალითი. როდესაც პროცესი იწყება პრობლემების ამოცნობით და ტექნიკურ და ადამიანურ გადაწყვეტილებებში ინვესტიციით, სადაც უსაფრთხოება არ არის იგნორირებული, არამედ პირველ ადგილზეა. მაგალითად, კიბერუსაფრთხოების გუნდის თანამშრომლების აყვანით და საბიუჯეტო ინვესტიციებით [„კიბერუსაფრთხოების საპასუხო ფონდში“](), პარლამენტი (და სხვა სამთავრობო ორგანოები) უკეთესად უნდა იყოს აღჭურვილი მომავალი თავდასხმების შესამცირებლად, თუ ასეთი რესურსები სათანადოდ გამოიყენება და გამძლეა და აქცენტი უნდა გაკეთდეს კიბერუსაფრთხოებაზე, როგორც საპარლამენტო ოპერაციების რეგულარულ შემადგენელ ელემენტზე. ამის გათვალისწინებით, რა თქმა უნდა, უკეთესია, რომ უსაფრთხოებაზე პასუხისმგებლობა პარლამენტში დანერგოთ *მანამდე სანამ* უსაფრთხოების მნიშვნელოვანი დარღვევა მოხდება.

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, თუმცა, 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 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 პარლამენტის მიღმა. ყოველივე ამის შემდეგ, მნიშვნელოვანია გვახსოვდეს, რომ პარლამენტის უსაფრთხოება ისეთივე საიემდო იქნება, როგორიც მისი ყველაზე სუსტი რგოლი. ერთ-ერთი მეთოდი თანამიმდევრული ჩართულობის მისაღწევად არის უსაფრთხოების შეტანა რეგულარული კრებების დღის წესრიგში. ასევე, შეგიძლიათ, გაუნაწილოთ უსაფრთხოების თაობაზე დისკუსიის ორგანიზების და ფასილიტაციის პასუხისმგებლობა პარლამენტის წევრებს, რამაც შესაძლოა წარმოშვას აზრი, რომ უსაფრთხოების დაცვა არის არა მხოლოდ რამდენიმე თანამშრომლის ან IT-გუნდის, არამედ ყველას პასუხისმგებლობა. 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 უსაფრთხოების ელემენტების ჩართვა პარლამენტის ნორმალურ ფუნქციონირებაში, მაგალითად, წევრებისა და პერსონალის სამსახურში აყვანის დროს და სისტემებზე წვდომის გამორთვა სამსახურიდან გათავისუფლების დროს. უსაფრთხოება არ უნდა იყოს რაღაც „დამატებითი“ წუხილის საგანი, არამედ უნდა იყოს **თქვენი სტრატეგიის და ოპერაციების განუყოფელი ნაწილი.**

გახსოვდეთ, რომ უსაფრთხოების ყველა გეგმა უნდა აღიქმებოდეს, როგორც ცოცხალი დოკუმენტი და რეგულარულად უნდა ხდებოდეს მისი განხილვა, განსაკუთრებით უსაფრთხოების კონტექსტის ცვლილების შემთხვევაში.

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

მიიღეთ ორგანიზაციული თანხმობა

წარმატებული უსაფრთხოების კულტურის ნაწილია ასევე თქვენი უსაფრთხოების გეგმის პარლამენტის მიერ დამტკიცება.

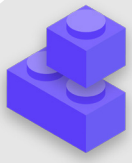
მეტად მნიშვნელოვანია, რომ აღნიშნული მოიცავდეს პარლამენტის ხელმძღვანელობის ხმამაღალ მხარდაჭერას და მითითებებს, რომლებიც ბევრ შემთხვევაში საბოლოო გადაწყვეტილებას მიიღებენ დროის, რესურსების და ენერგიის გამოყოფაზე უსაფრთხოების ეფექტური გეგმის შემუშავების მიზნით. თუ არა ისინი, ამას არც სხვა აღიქვამს სერიოზულად. ორგანიზაციის ხსენებული ჩართულობის მისაღწევად გულდასმით დაფიქრდით როდის და როგორ წარმოადგინოთ თქვენი გეგმა, გააკეთეთ ეს ნათლად, უზრუნველჰყავით, რომ ხელმძღვანელობა მხარს უჭერდეს თქვენს შეხედულებებს და გააცანით ყველას გეგმის ყველა ელემენტი და ნაბიჯი ისე, რომ თქვენი მიზანი არ იყოს საიდუმლო ან ბუნდოვანი. დარწმუნდით, რომ ბიუჯეტი მოიცავს პარლამენტის ადექვატურ კიბერუსაფრთხოებას. მიუხედავად იმისა, რომ ფინანსები შეიძლება შეზღუდული იყოს, მნიშვნელოვანია კიბერუსაფრთხოებაში ინვესტიციის სწორად განხორციელება, წინააღმდეგ შემთხვევაში სხვა ინვესტიციები შეიძლება საფრთხის ქვეშ დადგეს. უსაფრთხოებაზე საუბრისას მოერიდეთ შეშინების ტაქტიკას. ხანდახან საფრთხეები, რომელთა წინაშეც თქვენი პარლამენტი 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 მოთხოვნა და ტრენინგზე სავალდებულო დასწრება შეიძლება იყოს სასარგებლო ტაქტიკა. 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 პარლამენტში 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.

იფიქრეთ იმაზე, თუ როგორ შეიძლება თქვენი სასწავლო გეგმის გაცნობა პარლამენტის წევრების, პარლამენტის თანამშრომლების და პარლამენტის ადმინისტრაციისთვის. გაითვალისწინეთ, რომ გამოჩენილი წევრები ხშირად საჭიროებენ უფრო მეტ ტრენინგს და ყურადღებას, როდესაც საქმე ეხება უსაფრთხოებას მათი მაღალი სტატუსის გამო. დარწმუნდით, რომ თქვენი ტრენინგისა და უსაფრთხოების გეგმა მოიცავს ყველა ამ სხვადასხვა ტიპის პიროვნებას და აქტივებს, რომელიც მათ შეიძლება ჰქონდეთ პარლამენტის შიგნით და გარეთ.



უსაფრთხოების კულტურის დანერგვა

- **დაგეგმეთ რეგულარული საუბრები და ტრენინგი უსაფრთხოების და თქვენი უსაფრთხოების გეგმის შესახებ.**
- **ჩართეთ ყველა – გაანაწილეთ პასუხისმგებლობა თქვენი უსაფრთხოების გეგმის შესრულებაზე მთელს პარლამენტში.**
- **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 უსაფრთხოების გეგმა ყოველწლიურად ან პარლამენტის პერსონალის, სტრუქტურის ან საოპერაციო გარემოს მნიშვნელოვანი ცვლილებების შემდეგ.**

მყარი საფუძველი: ანგარიშებისა და მოწყობილობების დაცვა

რატომ კეთდება აქცენტი ანგარიშებსა და მოწყობილობებზე? რადგან ისინი ქმნიან ყველაფრის საფუძველს, რასაც თქვენი პარლამენტი ციფრულად აკეთებს.

თქვენ თითქმის სისტემატიურად გაქვთ წვდომა სენსიტიურ ინფორმაციაზე, ურთიერთობთ პარლამენტის შიგნით და გარეთ და ინახავთ მათზე პერსონალურ ინფორმაციას. უბრალოდ წარმოიდგინეთ წევრების მონაწილეობა პლენარულ სხდომებში, კენჭისყრაში (მათ შორის ვირტუალურ), კანონპროექტის შემუშავების პროცესებში და თანამშრომლებთან და ფართო საზოგადოებასთან კომუნიკაციის დროს. უსაფრთხო ანგარიშებისა და მოწყობილობების გარეშე, ეს კრიტიკული საპარლამენტო ოპერაციები და სხვა შეიძლება რისკის ქვეშ დადგეს. 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 მეტოქე მოიპოვებს წვდომას პარლამენტის სოციალური მედიის თქვენს ანგარიშებზე, მას შეუძლია ადვილად დააზიანოს თქვენი რეპუტაცია და სანდოობა, რაც ძირს უთხრის საზოგადოების ნდობას. ამდენად, როგორც პარლამენტმა, 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 ხალისით ეძებენ ადვილ სამიზნეს და გატეხენ პერსონალურ ანგარიშს ან სახლის კომპიუტერს, თუ თქვენი გუნდის წევრები იყენებს მათ კომუნიკაციის და მნიშვნელოვან ინფორმაციაზე წვდომისათვის.

უსაფრთხო ანგარიშები და პარლამენტები

ფართოდ გაშუქებული SolarWinds-ის 2020 წლის ბოლოს გამოვლენილი გატეხა, რომელმაც დააზარალა 250-ზე მეტი ორგანიზაცია, მათ შორის, შეერთებული შტატების დეპარტამენტები, Microsoft-ის და Cisco-ს მსგავსი ტექნოლოგიის მიმწოდებლები და არასამთავრობო ორგანიზაციები, ნაწილობრივ გამოწვეული იყო **ჰაკერების მიერ მარტივი პაროლების გამოცნობით**, რომლებიც გამოიყენებოდა მნიშვნელოვან ადმინისტრაციულ ანგარიშებში. 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 ყველა ორგანიზაციისთვის, მათ შორის პარლამენტისთვის. არც ერთი ინციდენტი არ ასახავს ამას უფრო ნათლად, ვიდრე **2017 თავდასხმა** ბრიტანეთის პარლამენტის ელექტრონული ფოსტის სისტემაზე. ამ ინციდენტში პაროლების არასწორად გამოყენებამ დეპუტატების მცირე, მაგრამ მნიშვნელოვანი რაოდენობის მიერ გამოიწვია ელფოსტისა ანგარიშებისა და საუბრის გამჟღავნება, ათასობით რწმუნებათა სიგელის გაჟონვა და პარლამენტის ფუნქციონირების კრიტიკული შეფერხება. ბრიტანეთის პარლამენტის პრეს-სამსახურის**მიხედვით**, ანგარიშები „გატეხილია სუსტი პაროლების გამო, რომლებიც არ ემორჩილებოდა პარლამენტის ციფრული სამსახურის მიერ გაცემულ მითითებებს“.

უსაფრთხო ანგარიშები: პაროლები და ორფაქტორიანი ავთენტიკაცია

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

იფიქრეთ სხვადასხვა ანგარიშზე, რომლებიც შეიძლება ჰქონდეთ პერსონალის წევრებს და მთლიანად პარლემენტს: ელ-ფოსტა, 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 პაროლის კარგი ჰიგიენით და ყველას მიერ ორფაქტორიანი ავთენტიფიკაციის გამოყენებით.

როგორია კარგი პაროლი?

კარგ, ძლიერ პაროლს განაპირობებს სამი ფაქტორი: სიგრძე, შემთხვევითობა 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.
შემთხვევითობა	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, შემთხვევითობისა 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 **ეს ვებსაიტი** და გაეცნოთ პროგნოზს, რამდენად სწრაფად შეიძლება სუსტი პაროლის გატეხვა.

დახმარებისათვის გამოიყენეთ პაროლების მენეჯერი

მაშ, თქვენ იცით, რომ მნიშვნელოვანია ყველამ პარლამენტში გამოიყენოს გრძელი, შემთხვევითი და განსხვავებული პაროლი თითოეული მათი პერსონალური და საპარლამენტო ანგარიშისთვის, მაგრამ რას აკეთებთ 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 ანგარიშზე პარლამენტში დაცული პაროლების გაზიარების გამარტივების მიზნით.

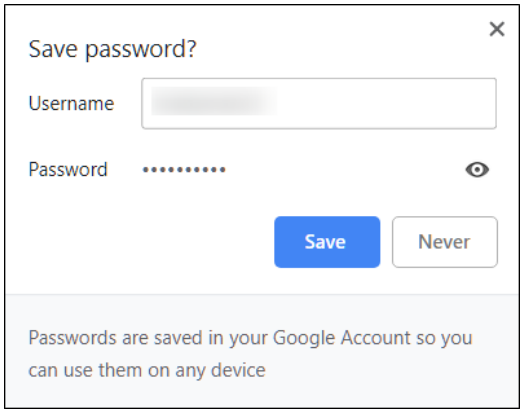
რატომ გვჭირდება რაღაც ახლის გამოყენება? არ შეგვიძლია უბრალოდ ჩამოვწეროთ ისინი ქაღალდზე ან კომპიუტერულ ცხრილში?

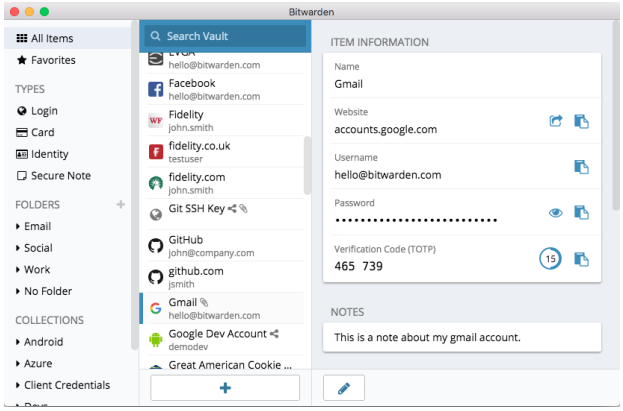
სამწუხაროდ, არსებობს მრავალი გავრცელებული მიდგომა პაროლების მართვისადმი, რომლებიც არაა უსაფრთხო. ქაღალდის ფურცლებზე პაროლების შენახვამ (თუ არ ინახავთ მათ სეიფში ჩაკეტილს), შესაძლოა, დაუქვემდებაროს ისინი ფიზიკურ ქურდობას, ცნობისმოყვარე თვალს და უბრალოდ დაკარგვას ან დაზიანებას. პაროლების კომპიუტერულ დოკუმენტში 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 მენეჯერებს გააჩნია ფუნქცია აქციოს თქვენი პარლემენტის 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 მიუღებელია უსაფრთხოების თვალსაზრისით მიუღებელია. აღნიშნული ნაკლოვანებები ასევე გართმევთ კომფორტს, რომელიც თან სდევს კარგ პაროლების მენეჯერს. ამ კომფორტის დაკარგვა ზრდის იმის ალბათობას, რომ პარლამენტარი გააგრძელებს პაროლების გენერირებისა და გაცვლის არასწორი მეთოდების გამოყენებას.

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 პარლამენტის უსაფრთხოებისათვის. პაროლების მენეჯერი ასევე მოიცავს ორგანიზაციისათვის სპეციფიკურ ფუნქციებს (როგორიცაა პაროლის გაზიარება), რომლებიც უზრუნველყოფს არა მხოლოდ ინდივიდუალურ უსაფრთხოებას, არამედ მთელი თქვენი პარლამენტის უსაფრთხოებასაც. თუ პაროლენს თქვენს ბრაუზერში ინახავდით (გამიზნულად ან უნებლიედ), ნუ დაიზარებთ, წაშალოთ ისინი.

რომელი პაროლების მენეჯერი უნდა გამოვიყენოთ?

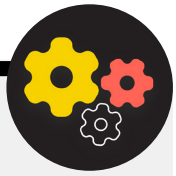
არსებობს არაერთი კარგი პაროლების მენეჯერი, რომელთა დაყენებაც 30 წუთზე ნაკლებ დროში შეიძლება. თუ ეძებთ სანდო ონლაინ ვარიანტს თქვენი პარლამენტისთვის, რომელზე წვდომაც ნებისმიერ დროს შეეძლება ხალხს არაერთი მოწყობილობიდან, სათანადოდ მხარდაჭერილი და რეკომენდებულია **1Password** (იწყება ერთ მომხმარებელზე თვეში 2,99 აშშ დოლარიდან) ან უფასო, ღია კოდის მქონე **Bitwarden**. Bitwarden-ის მსგავსი ონლაინ-ვარიანტი, შესაძლოა, შესანაშნავი იყოს როგორც უსაფრთხოების, ისე კომფორტულობის მხრივ. Bitwarden, მაგალითად, დაგეხმარებათ, შექმნათ ძლიერი უნიკალური პაროლები და იქონიოთ წვდომა პაროლებზე არაერთი მოწყობილობიდან ბრაუზერით თუ მობილურის აპით. Bitwarden-ის ფასიანი ვერსია (10 აშშ დოლ. წელიწადში)

ასევე გვატყობინებს ხელახლა გამოყენებულ, სუსტ ან სავარაუდოდ გატეხილ პაროლებზე, რათა იყოთ ყველა გარემოების საქმის კურსში. თქვენი პირველადი პაროლის (ხსენებული, როგორც გნერალური პაროლი) შექმნის შემდეგ ასევე უნდა ჩართოთ აუთენტურობის ორფაქტორული შემოწმება, რათა მაქსიმალურად დაცული იყოს თქვენი პაროლების დისპეტჩერის საცავი.

მაღალი დონის უსაფრთხოების **წარმართვა ასევე მნიშვნელოვანია პაროლების დისპეტჩერის 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 თქვენ პაროლებს აზიარებთ გუნდის წევრებს შორის ან მთლიანად პარლამენტს შორის, დარწმუნდით, რომ გააუქმეთ პაროლებზე წვდომა (და თავად შეცვალეთ პაროლები), როდესაც ვინმე წავა სამსახურიდან. მაგალითად, თქვენ არ გენდომებათ, რომ ყოფილ თანამშრომელს ჰქონდეს წვდომა თქვენს საპარლამენტო ფეისბუქის პაროლზე.

რა მოხდება, 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 ელ-ფოსტით შეცვლის საშუალებას გაძლევთ ისე, როგორც ვებსაიტებზე. ეს უსაფრთხოების მაღალი დონის ფუნქციაა, მაგრამ ასევე იძულებულს გხდით, დაიმახსოვროთ თქვენი პირველადი პაროლი პაროლების მენეჯერის დაყენების შემდეგ. ამ მიმართებაში დასახმარებლად, პაროლების დისპეტჩერის პაროლის პირველად შექმნისას, შესაძლოა გამართოთ ყოველდღიური შეხსენება თქვენი პირველადი პაროლისათვის.



პაროლის მენეჯერის გამოყენება თქვენი პარლამენტისთვის

შეგიძლიათ, გააუმჯობესოთ მთელს თქვენს პარლამენტში 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 აშშ დოლარი ღირს თვეში. მის (ან 1Password-ის მსგავსი პაროლების მენეჯერის მსგავსი სხვა გუნდური გეგმის) ხარჯზე გიჩნდებათ უნარი, მართოთ მთელს ორგანიზაციაში გაზიარებული ყველა პაროლი. პარლამენტის ან გუნდის პაროლის მენეჯერის ფუნქციები არა მხოლოდ უფრო მეტ უსაფრთხოებას, არამედ კომფორტს უზრუნველყოფს 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 პარლამენტს 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 საპარლამენტო 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. 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 პარლამენტში ასე მნიშვნელოვანი.

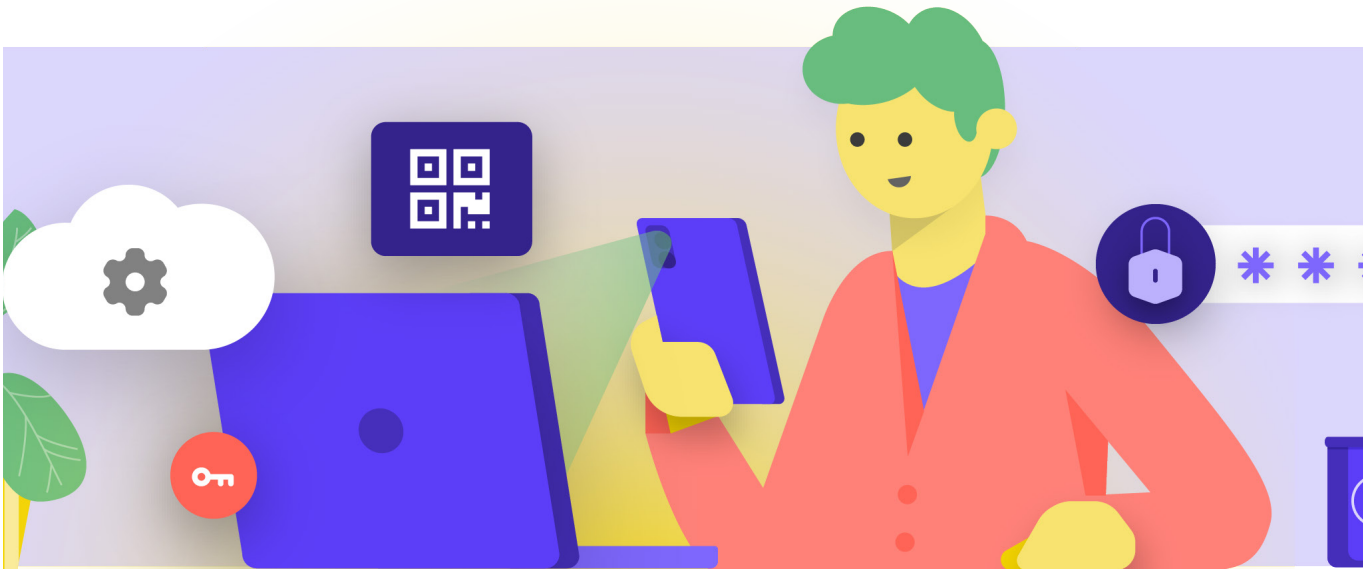
ერთი სიტყვით, 2FA აამაღლებს ანგარიშის დაცულობას, მოითხოვს რა წვდომის მისაღებად მეორად ინფორმაციას – რაღაც მეტს, ვიდრე მხოლოდ პაროლს. მეორადი ინფორმაცია, ჩვეულებრივ, არის რაღაც ისეთი, როგორიცაა აპლიკაციის კოდი თქვენს ტელეფონში, ფიზიკური ნიშანი ან გასაღები.
ხსენებული მეორადი ინფორმაცია ასრულებს დაცვის 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). მნიშვნელოვანია იმის უზრუნველყოფა, რომ პარლამენტში ყველას ჰქონდეს 2FA დაინსტალირებული საკუთარ ანგარიშებზე.

როგორ დავაყენოთ 2FA?

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

დამცავი გასაღებები

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 აშშ დოლარი), მათ შორის, მაღალი შეფასების მქონე **YubiKeys-ი**. „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.



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

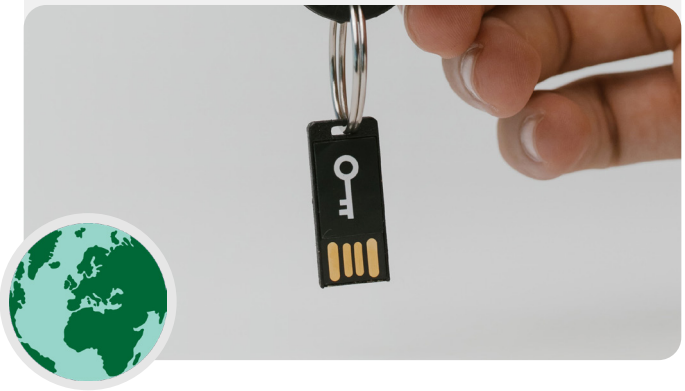
2FA-ს ყველაზე დაუცველი, მაგრამ სამწუხაროდ ყველაზე გავრცელებული ფორმაა SMS-ით კოდების გაგზავნა. რამდენადაც SMS, შესაძლოა, იქნეს ხელში ჩაგდებული, ხოლო ტელეფონის ნომერი – იმიტირებული ან გატეხილი თქვენი მობილური ოპერატორის მეშვეობით, SMS ჯერ კიდევ მიუღებელია, როგორც 2FA-ს კოდების მოთხოვნის მეთოდი. ეს უკეთესია,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

2FA და პარლამენტები

2020 წლის ანგარიშების თანახმად, **ჰაკერებმა შეაღწიეს ნორვეგიის პარლამენტის ელეფოსტის სისტემაში.** გატეხეს ელფოსტის ანგარიშები, რომლებიც ეკუთვნოდა პარლამენტის რამდენიმე თანამდებობის პირს და ჩამოტვირთეს გარკვეული ინფორმაცია საპარლამენტო სისტემებიდან. მიუხედავად იმისა, რომ ჰაკერის სრული დეტალები არ იყო საჯარო, ნორვეგიამ შეჭრა მიაწერა APT28-ს, ჰაკერულ ჯგუფს, რომელიც კავშირშია რუსეთის უსაფრთხოების სამსახურებთან. მიუხედავად მათი დახვეწილობისა, APT28 და სხვა ჰაკერები ხშირად იყენებენ ნაკლებად დახვეწილ ტაქტიკას, როგორიცაა „უხეში ძალის შეტევები“ (სადაც თავდამსხმელი იყენებს ინსტრუმენტებს უხეში ძალის გამოყენებით მრავალი პაროლის გამოსაცნობად) ანგარიშზე წვდომის მისაღებად. ეს ტაქტიკა ჰაკერებს საშუალებას აძლევს გამოიცნონ ძლიერი პაროლებიც კი, როგორიცაა ნორვეგიაში. კარგი ამბავია? ამ ტიპის შეტევები გაცილებით ნაკლებად წარმატებულია სათანადო გასაღების ან აპზე დაფუძნებული ორფაქტორიანი ავთენტიფიკაციის გამოყენების შემთხვევაში!

დამცავი გასაღებები რეალურ სამყაროში

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



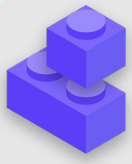
რა მოხდება, თუ ვინმე დაკარგავს 2FA-ს მოწყობილობას?

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. დარწმუნდით, რომ ყველამ იცის ეს ნაბიჯები, რადგან ისინი დაიწყებენ 2FA-ს ჩართვას ყველა ანგარიშზე.

2FA-ის გამოყენება თქვენს პარლამენტში

თუ თქვენი პარლამენტი უქმნის ელ-ფოსტის 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 პერსონალურ 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.



უსაფრთხო ანგარიშები

- **მოითხოვეთ ძლიერი პაროლები ყველა საპარლამენტო ანგარიშისთვის; გააკეთეთ იგივე წევრების, პერსონალის და მოხალისეების პირადი ანგარიშებისთვის.**
- **დანერგეთ ძლიერი საპარლამენტო პაროლის მენეჯერი (და წაახალისეთ მისი გამოყენება თანამშრომლების პირად ცხოვრებაში).**
  - 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 გაზიაირებული პაროლები, როდესაც თანამშრომლები და წევრები ტოვებენ პარლამენტს.**
- **გააზიარეთ პაროლები მხოლოდ უსაფრთხო გზით, მაგალითად, თქვენი პარლამენტის პაროლის მენეჯერის ან თავიდან ბოლომდე დაშიფრული აპების მეშვეობით.**
- **მოითხოვეთ ორფაქტორიანი ავთენტიფიკაცია ყველა საპარლამენტო ანგარიშისთვის და წაახალისეთ თანამშრომლები, დააყენონ ორფაქტორიანი ავთენტიფიკაცია ყველა პირადი ანგარიშისთვისაც.**
  - თუ შესაძლებელია, მიაწოდეთ ფიზიკური უსაფრთხოების გასაღებები ყველა მონაწილესა და პერსონალს.
  - 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.

ეს დაცვა იწყება სიფრთხილის გამოჩენით, თუ რა მოწყობილობებს ყიდულობენ და იყენებენ თქვენი პარლამენტი და თანამშრომლები. 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 საფუძველი 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 ტექნიკის ღირებულება შეიძლება მოგეჩვენოთ ძალიან მიმზიდველი, პარლამენტებისთვის უსაფრთხოების პოტენციური რისკები უნდა გაგიმხნევოთ, აირჩიოთ სხვა ტექნიკისა და ტექნიკის ვარიანტები.

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 პარლამენტები

ზოგიერთი ყველაზე მოწინავე მავნე პროგრამა შემუშავებულია და განლაგებულია მთელ მსოფლიოში, რათა [სამიზნე](#) მიესაჯა დეპუტატებს, სხვა სახელმწიფო მოხელეებს და მათ თანამშრომლებს. მაგალითად, ინდოეთში, ჟურნალისტთა კონსორციუმმა [გამოავლინა](#), რომ რამდენიმე დეპუტატი და მთავრობის მინისტრი იყო Pegasus spyware-ის მსხვერპლი, მავნე პროგრამის ტიპი, რომელიც 2020 წელს გახდა სათაურები. პეგასუსი ცნობილია მობილური მოწყობილობების დაინფიცირების უნარით და დამნაშავეს აუდიოს ჩაწერის, კლავიშებისა და შეტყობინებების ჩასმის უნარით და არსებითად მსხვერპლს სრული მეთვალყურეობის ქვეშ , დაზარალებულის ჩარევის გარეშე. თუმცა, ჯაშუშური პროგრამების აბსოლუტური უმრავლესობა ახერხებს მსხვერპლთა კომპრომეტირებას.

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 დაგჭირდებათ საიმედო საკეტების, უსაფრთხოების კამერების ან სხვა სათვალთვალო სისტემების დაყენება. 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. დარწმუნდით, რომ პარლამენტის მიერ გაცემული ყველა მოწყობილობა ასევე რეგისტრირებულია **მობილური მოწყობილობების მართვის ან საბოლო წერტილის მართვის სისტემაში.** მიუხედავად იმისა, რომ ეს სისტემები არის იაფი, ისინი თქვენს პარლამენტს საშუალებას აძლევს განახორციელოს უსაფრთხოების პოლიტიკა ყველა მოწყობილობაზე, აღმოაჩინოს ერთი და წაშალოს მისი პოტენციურად მგრძნობიარე კონტენტი, თუ ის მოიპარება, დაკარგავს ან ჩამოართმევს. მიუხედავად იმისა, რომ არსებობს მრავალი განსხვავებული მობილური მოწყობილობების მართვის გადაწყვეტილებები, რამდენიმე სანდო ვარიანტი, რომლებიც მუშაობს სხვადასხვა პლატფორმებზე (iPhone, Android, Mac და Windows) მოიცავს Hexnode, Cisco Meraki Systems Manager, IBMs MDM და ჩაშენებული Google Workspace მობილური მოწყობილობების მართვა. თუ ღირებულება შემაკავებელი ფაქტორია, სულ მცირე, წაახალისეთ წევრები და თანამშრომლები, გამოიყენონ ჩაშენებული “იპოვე ჩემი მოწყობილობა“ ფუნქციები მათ პარლამენტში გაცემულ და პერსონალურ სმარტფონებზე, როგორიცაა Find My iPhone-ზე და Find My Device Android-ზე.

რას იტყვით მოწყობილობის დაშიფვრაზე?

მნიშვნელოვანია ყველა მოწყობილობაში, განსაკუთრებით კომპიუტერებში და სმარტფონებში, გამოვიყენოთ მონაცემთა დაშიფვრა, სკრემბლინგი ისე, რომ ის შეიქნას არაკითხვადი და უსარგებლო. თქვენ უნდა დააყენოთ ყველა მოწყობილობაზე პარლამენტში, **სრული დისკის დაშიფვრა** , თუ ეს შესაძლებელია. დისკის სრულად დაშიფვრა გულისხმობს, რომ მოწყობილობის მთელი დისკი დაშიფრულია ისე, რომ, თუ ქურდობის საგნად იქცევა, დამნაშავეებს 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 კომპიუტერებისთვის, 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 უსაფრთხოებას. 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 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 მომდევნო ნაწილში.

საზიანო პროგრამის ინტერპრეტაცია და თავიდან აცილება

არსებობს საზიანო პროგრამის (რომელიც, განსაზღვრების თვალსაზრისით, წარმოადგენს საზიანო პროგრამულ უზრუნველყოფას) კლასიფიკაციის არაერთი გზა. ვირუსები, სათვალთვალო 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 შეუძლია, 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.

რაც არ უნდა ერქვათ მათ, როგორიც კი ისინი გავრცელდება, მავნე პროგრამას შეუძლია გაანადგუროს კომპიუტერები, მოიპაროს და გაანადგუროს მონაცემები, შეაყოვნოს პარლამენტის მუშაობა, შეიჭრას კონფიდენციალურობა და საფრთხე შეუქმნას მომხმარებლებს. ერთი სიტყვით, საზიანო პროგრამული უზრუნველყოფა მართლაც სახიფათოა. თუმცა, არსებობს რამდენიმე მარტივი ნაბიჯი, რომელიც თქვენს პარლამენტს შეუძლია გადადგას ამ საერთო საფრთხისგან 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 ასეტ ინსტრუმენტზე დაყრდნობა ვერ იქნება დაცვის თქვენი ერთადერთი საშუალება.

თუ იყენებთ Windows-ს უნდა გაცნობოდით WindowsDefender-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,** მათ აუცილებლად გამოეპარებათ ზოგიერთი ყველაზე მიზნობრივი და სახიფათო ახალი შეტევა.

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.

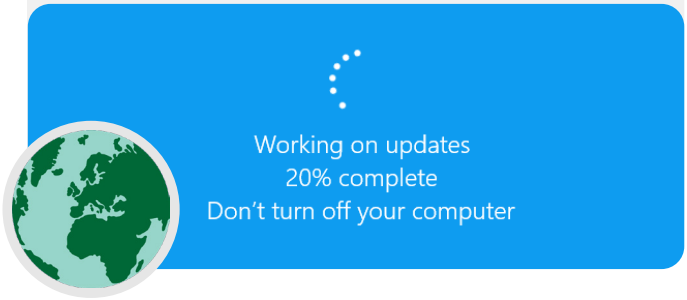
თუ თქვენს პარლამენტში Bitdefender-ს ან საზიანო პროგრამების საწინააღმდეგო სხვა ხელსაწყოს იყენებთ, ორი მათგანი ერთდროულად არ უნდა ჩართოთ. არაერთი მათგანი აღიქვამს მეორე ანტი-საზიანო პროგრამული უზრუნველყოფის ქცევას საეჭვოდ და აჩერებს მის მუშაობას რაც იწვევს ორივეს გაუმართაობას. Bitdefender ან საზიანო პროგრამების 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 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 დაკავშირებული 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.

საზიანო პროგრამული უზრუნველყოფა რეალურ სამყაროში: მავნე მობილური აპლიკაციები

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.

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. 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.

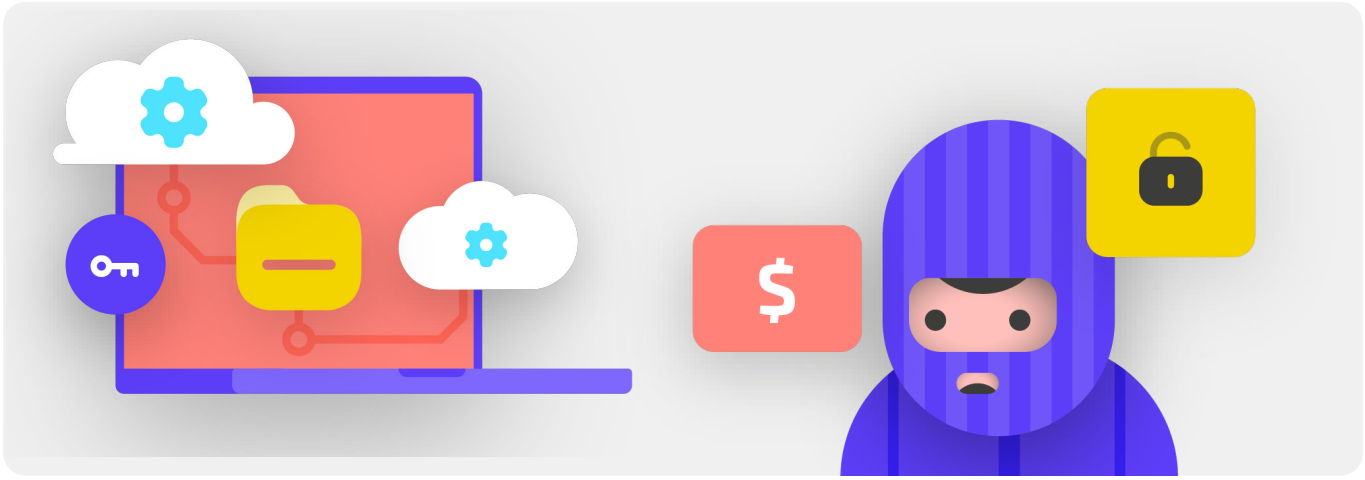
მოწყობილობის უსაფრთხოდ შენახვა

- **აცნობეთ მონაწილეებს და თანამშრომლებს მავნე პროგრამების რისკების შესახებ და მისი თავიდან აცილების საუკეთესო 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.
- **ჩართეთ ყველა საპარლამენტო მოწყობილობა თქვენს მობილურ მოწყობილობაში ან საბოლოო წერტილის მართვის სისტემაში.**
- **დარწმუნდით, რომ ყველა მოწყობილობაზე გამოიყენებოდეს ლიცენზირებული პროგრამული უზრუნველყოფა.**
- **მოითხოვეთ პაროლით დაცვა ყველა საპარლამენტო მოწყობილობისთვის, მათ შორის პერსონალური მობილური მოწყობილობებისთვის, რომლებიც გამოიყენება საპარლამენტო კომუნიკაციების დროს.**
- **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 არის ყველაზე გავრცელებული და ეფექტური შეტევა ორგანიზაციებზე, მათ შორის პარლამენტებზე, მთელ მსოფლიოში. 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 ეცოდონ 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. შემდეგი ანტიფიშინგის რჩევები შეცვლილია და გავრჩობილია [Free Press Foundation](#)-ის დეტალური ანტიფიშინგის სახელმძღვანელოდან, ის უნდა გააცნოთ ყველას პარლამენტში და მის გარეთ და შეიყვანოთ 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@goooogle.com" ნაცვლად „john@google.com”-ისა. 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 გახნამდე. მსგავსი კონცეფცია ეხება ფიშინგს ტექსტის, ზარების თუ მესინჯერი აპების საშუალებით. თუ მიიღებთ შეტყობინებას უცნობი ნომრიდან, დაფიქრდით ორჯერ პასუხის გაცემამდე ან შეტყობინებაზე ინტერაქციამდე.

ფიშინგი და პარლამენტები

დახვეწილი, პერსონალიზებული ფიშინგ შეტევები რეგულარულად მიზანში იღებს პარლამენტებს და სხვა სამთავრობო უწყებებს მთელს მსოფლიოში.

გერმანიის ფედერალური და ადგილობრივი პარლამენტის ოფიციალური პირები 2021 წლის შემოდგომის წინასაარჩევნო პერიოდში ელფოსტის ფიშინგის სამიზნე გახდნენ. სულ რაღაც რამდენიმე თვით ადრე, ავღანეთში, ჰაკერულმა ჯგუფმა [ფიშინგის ტექნიკა გამოიყენა ყოფილ ეროვნული უშიშროების საბჭოში](#) წარმატებით შესაღწევად, ავღანეთის ყოფილი პრეზიდენტის აშრაფ ღანის სპიკერის ვინაობის დასადგენად.

ჰაკერებმა გაგზავნეს ფიშინგ ელწერილი (ზემოთ არის ნაჩვენები), რომელიც მსხვერპლს სთხოვდა გაეხსნა თანდართული ფაილი, რომელიც სპიკერის მტკიცებით შეიცავდა შეცდომას. როდესაც მსხვერპლებმა ჩამოტვირთეს და გახსნეს ფაილი „შეცდომის შესამოწმებლად“, მავნე დანართმა გაუშვა მავნე პროგრამა, რომელიც ჰაკერებს მუდმივ წვდომას აძლევდა კომპიუტერებზე. ეს წვდომა საშუალებას აძლევდა ჰაკერებს აეტვირთათ და ჩამოეტვირთად ფაილები, სურვილისამებრ გაეშვათ ბრძანებები მოწყობილობებზე და მოეპარათ მგრძნობიარე სახელმწიფო მონაცემები.

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 „ღდამატებით" 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;

პარლამენტის ფისინგისგან დაცვა

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** ეწოდება. უფრო გამოცდილ ინდივიდუალურ მომხმარებლებს შეუძლიათ იფიქრონ რთული სენდბოქს პროგრამების გამართვაზე, როგორიცაა **Dangerzone**ან, მათთვის, ვისაც აქვთ Windows 10-ის პრო- ან კორპორაციული ვერსია, **Windows Sandbox**. კიდევ ერთი მოწინავე ვარიანტი, რომელიც გასათვალისწინებელია პარლამენტში განსახორციელებლად, ეს არის უსაფრთხო დომენის სახელების სისტემის (DNS) ფილტრაციის სერვისი.

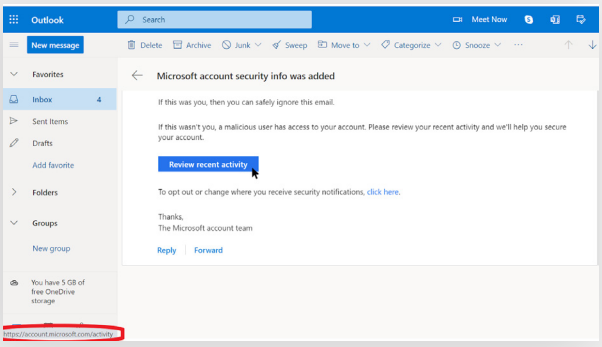
ორგანიზაციებს შეუძლიათ გამოიყენონ ხსენებული ტექნოლოგია, რათა დაბლოკონ მასალა შემთხვევით დაშვებული ან ინტერაქციაში მოხვედრილი საზიანო კონტენტიდან, რაც იძლევა ფიშინგისაგან დაცვის დამატებით შრეს. ახალი სერვისები, როგორიცაა **Cloudflare's Gateway** გთავაზობთ ამ შესაძლებლობების დაყენებას დიდი თანხების საჭიროების გარეშე. დამატებითი უფასო ინსტრუმენტები, მათ შორის, Global Cyber Alliance-ის კომპლექტის **Quad9** 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.

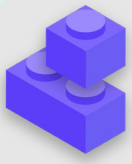
და ბოლოს, თუ დააწკაპუნებთ შეტყობინებაში მოცემულ ნებისმიერ ბმულზე და გთხოვენ შეხვიდეთ რომელიმე



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 პარლამენტში მიიღებს არასასურველ დანართს, ბმულს, სურათს ან სხვა საეჭვო შეტყობინებას ან სატელეფონო ზარს, მნიშვნელოვანია, რომ დაუყოვნებლივ აცნობოთ ამის შესახებ პასუხისმგებელ პირ(ებ)ს ან IT უსაფრთხოების ჯგუფს. თუ არ გყავთ ასეთი პირი, უნდა გამოყოთ ასეთი პირი უსაფრთხოების თქვენი გეგმის შემუშავების პროცესში. თანამშრომლებსა და წევრებს ასევე შეუძლიათ აცნობონ ელფოსტის შეტყობინების შესახებ, როგორც სპამი ან ფიშინგი პირდაპირ Gmail ან Outlook-იდან.
უმნიშვნელოვანესია იქონიოთ გეგმა, თუ როგორ უნდა მოიქცეს პერსონალი ან მოხალისეები, როდესაც მიიღებენ შესაძლო ფიშინგ შეტყობინებას. გარდა ამისა, გირჩევთ მიიღოთ 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 იმისა, რომ ზემოაღნიშნული რჩევები ყველას გაუზიარებთ, ასევე შეგიძლიათ ივარჯიშოთ ფიშინგის იდენტიფიცირებაზე Google Phishing Quiz დახმარებით. ასევე დაბეჯითებით გირჩევთ გამართოთ პერსონალის რეგულარული ტრენინგი ფიშინგის საკითხებზე, რათა შემოწმდეს ინფორმირებულობა, ხოლო ხალხი იყოს ფხიზლად. ასეთი ტრენინგი შეიძლება ფორმალიზებული იყოს რეგულარული გუნდისა და საპარლამენტო შეხვედრების გზით, ან ჩატარდეს უფრო არაფორმალურ გარემოში. მნიშვნელოვანია, რომ ყველა, ვინც მონაწილეობს საპარლამენტო ოპერაციებში, თავს კომფორტულად გრძნობდეს და დასვას კითხვები ფიშინგზე, ფიშინგის შეტყობინებაზე (მაშინაც კი, თუ ფიქრობენ, რომ შესაძლოა შეცდომა დაუშვეს, მაგალითად, ბმულზე დააწკაპუნეს) და ყველას აქვს უფლება დაეხმაროს ამ მაღალი ზემოქმედებისა და მაღალი ალბათობის საფრთხისგან პარლამენტის დაცვაში.



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 მონაწილეებს და თანამშრომლებს საუკეთესო პრაქტიკის 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.**
  - პარლამენტში ანგარიშგების მექანიზმის და ფიშინგის ოფიცრის ჩამოყალიბება.
  - წაახალისეთ რეპორტინგი და ნუ დასჯით წარუმატებლობისას.

Communicating and Storing Data Securely

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 საპარლამენტო კომუნიკაციები ხილული იქნება ნებისმიერი რაოდენობის ოპონენტისთვის. დაუცველმა კომუნიკაციამ შესაძლოა კონფიდენციალურობის 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. ასევე მნიშვნელოვანია პარლამენტმა უზრუნველყოს, რომ წევრებისა და თანამშრომლების ოფიციალური სამთავრობო კომუნიკაციები შეესაბამებოდეს მთავრობის ყველა შესაბამის ღია ვალდებულებას (როგორიცაა ინფორმაციის თავისუფლების მოთხოვნა) და მონაცემთა უსაფრთხოების ვალდებულებები. ამიტომ, პარლამენტში უსაფრთხო საკომუნიკაციო სისტემებისა და პოლიტიკის შემუშავებისა და დანერგვის დროს, აუცილებლად გასათვალისწინებელია ეს ფაქტორები, რათა სათანადო გზავნილები იყოს დაცული და კანონის მოთხოვნის შემთხვევაში, შენახული.

უსაფრთხო კომუნიკაციები და პარლამენტები

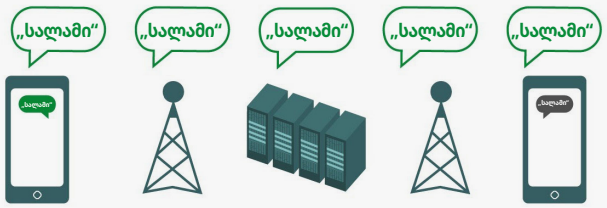
ბოლო წლებში ადგილი ქონდა ბევრ შემთხვევას, როდესაც პარლამენტების საკომუნიკაციო სისტემები და დეპუტატებისა და მათი თანამშრომლების ანგარიშები იყო გატეხილი, რამაც პარლამენტის მუშაობაში შეფერხება გამოიწვია და, ზოგიერთ შემთხვევაში, საიდუმლო შეტყობინებების მოპარვა მოხდა. მაგალითად, 2021 წლის ივლისში, პოლონეთის ხელისუფლებამ გამოაცხადა, რომ თითქმის ათეული ადგილობრივი დეპუტატისელფოსტის მისამართი იქნა გატეხილი, მათ შორის პრემიერ-მინისტრის მთავარი თანაშემწის პირადი ანგარიში და თითქმის ყველა საპარლამენტო ოპოზიციური ჯგუფის წევრების ანგარიშები. ეს შეტყობინება ცნობილი გახდა რამდენიმე თვის შემდეგ, როდესაც მსგავსი ამბები ფინეთის პარლამენტის საინფორმაციო და საკომუნიკაციო სისტემებზე კიბერშეტევის შესახებ გავრცელდა. ფინეთის ხელისუფლებამ შეტევა დაახასიათა, როგორც „ჯაშუშობა დამამძიმებელ გარემოებაში და შეტყობინებების მოპარვა" პარლამენტის წინააღმდეგ მიმართული.

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

ყოველგვარი დაშიფვრის გარეშე, ჩვენი კომუნიკაციები ღია რჩება პოტენციური მოწინააღმდეგეებისთვის, მათ შორის მტრულად განწყობილი უცხოური მთავრობების ან ინტერნეტ ჰაკერებისთვის. ასეთი დაშიფვრა მნიშვნელოვანია არა მხოლოდ შიდა საპარლამენტო კომუნიკაციებისთვის, არამედ გარე კომუნიკაციებისთვისაც, სადაც დაცული უნდა იყოს კონფიდენციალობა და მთლიანობა.

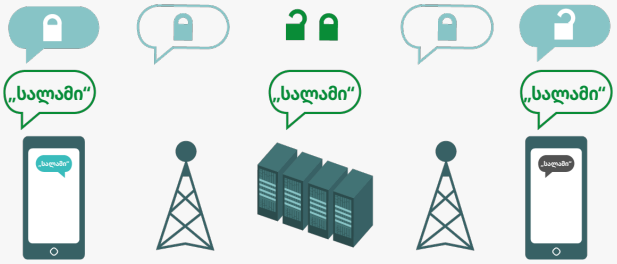


როგორც ზედა სურათზე ჩანს, სმარტფონი უგზავნის მწვანე, დაუშიფრავ ტექსტურ შეტყობინებას („სალამი“) მეორე, ბოლო მარჯვენა სმარტფონს. გზაში ფიჭური კავშირის ანძა (ან, რაიმეს ინტერნეტით გაგზავნისას, თქვენი ინტერნეტ-პროვაიდერი, რომელსაც ISP ეწოდება) გადასცემს შეტყობინებას კომპანიის სერვერებით. აქედან ის ქსელის 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 აღწერილი **„თვალთვალისაგან თავდაცვის სახელმძღვანელოს“** მიერ, რომელიც კვლავ ადაპტირებულია ქვემოთ:

სატრანსპორტო შრის დაშიფვრა

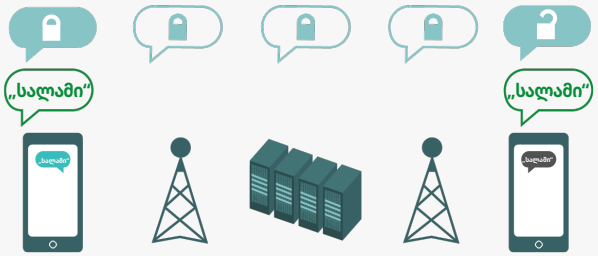
სატრანსპორტო შრის დაშიფვრა ასევე ცნობილი, როგორც სატრანსპორტო შრის უსაფრთხოება (TLS), იცავს შეტყობინებებს მათი თქვენი მოწყობილობიდან მესინჯერის სერვერებამდე და მათგან მიმღების მოწყობილობამდე მოძრაობის დროს. ეს იცავს მათ თქვენს ქსელში ან თქვენს ინტერნეტ- თუ ტელეკომუნიკაციის სერვისის პროვაიდერებთან მყოფი 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.

კიდევ ერთი საკითხი, რომელიც გასათვალისწინებელია, ის არის,რომ თქვენ, როგორც პარლამენტარს, კანონით თუ მოგეთხოვებათ, გქონდეთ ექსკლუზიური წვდომა ნებისმიერ საპარლამენტო კომუნიკაციაზე, არსებობს თუ არა რაიმე მოთხოვნა მონაცემთა ლოკალიზაციის შესახებ თქვენს ქვეყანაში და/ან თუ არის გარკვეული შეტყობინებები, რომელთა შენახვაც უნდა მოხდეს (მაგ. , პერსონალის მიერ არ უნდა მოხდეს სამუდამოდ წაშლა) მთავრობის მოქმედი კანონებისა და ვალდებულებების შესასრულებლად. თუ ასეა, უნდა განიხილოთ თავიდან ბოლომდე დაშიფრული საკომუნიკაციო სისტემა, სადაც თქვენ, როგორც პარლამენტარს, თავად შეგიძლიათ აკონტროლოთ დაშიფვრის გასაღებები. ასეთი სისტემები (რომლებიც უფრო დეტალურად იქნება განხილული სახელმძღვანელოს სექციაში **„მონაცემთა უსაფრთხო შენახვა“ შეიძლება იყოს საიმედო, მაგრამ განსახორციელებლად მოითხოვდეს მაღალ ტექნიკურ უნარებს.**

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.

რა ვუყოთ ელფოსტას?

ზოგადად, ელფოსტა არ არის საუკეთესო ვარიანტი, როდესაც საქმე ეხება უსაფრთხოებას. ელფოსტის დაშიფვრის საუკეთესო ვარიანტებიც კი, ზოგადად, ტოვებს უსაფრთხოების თვალსაზრისით გარკვეულ რისკებს როგორც მაგალითად ელფოსტის თემის ხაზების არ დაშიფვრა ან მეტამონაცემების არ დაცვა (მნიშვნელოვანი კონცეფცია, რომელიც ქვემოთ იქნება აღწერილი). თუ გჭირდებათ ძალიან სენსიტიური ინფორმაციის გადაცემა, რომელიც არ საჭიროებს საჯარო ჩანაწერებში შენახვას, გთხოვთ გაითვალისწინოთ, რომ უმჯობესია მოერიდოთ ამისთვის ელ ფოსტის გამოყენებას (როგორც საპარლამენტო სისტემიდან, ასევე ვინმეს პერსონალური ანგარიშიდან) ნაცვლად ისარგებლეთ უსაფრთხო შეტყობინებების ვარიანტებით (რომელიც აღწერილი იქნება შემდეგ ნაწილში).

თუმცა, როგორც პარლამენტს, შეიძლება მაინც გინდოდეთ ან გჭირდებოდეთ, რომ წევრები და პერსონალი, გადასცემდნენ ერთმანეთს სენსიტიურ ან კონფიდენციალურ მასალას გარკვეული სისტემის საშუალებით, რომელიც ცენტრალიზებულად იმართება, როგორც მათი ყოველდღიური ოპერაციების ნაწილი. პარლამენტის მასშტაბური ელფოსტის სისტემა, ანგარიშის სათანადო კონტროლით, რა თქმა უნდა, აქ შეიძლება სასარგებლო იყოს. თუ ზემოაღნიშნული ანალიზის მიხედვით, გამტარი ფენის დაშიფვრა საკმარისია, მაშინ სტანდარტული ბიზნეს შეთავაზებები ეფოსტის სერვისის პროვაიდერებისგან, როგორიცაა Google Workspace (Gmail) და Microsoft 365 (Outlook) თქვენი პარლამენტისთვის შეიძლება კარგი ვარიანტი იყოს. თუმცა, თუ ფიქრობთ, რომ თქვენი ელფოსტის პროვაიდერი შეიძლება სამართლებრივად ვალდებული იყოს, რომ გაუზიაროს თქვენი კომუნიკაციის შესახებ ინფორმაცია უცხო მთავრობას ან სხვა მეტოქეს, ან თუ ადგილობრივი მონაცემების შენახვის მოთხოვნები თქვენთვის მიუღებელია, თქვენ უნდა დაფიქრდეთ თავიდან ბოლომდე დაშიფრული ელფოსტის ვარიანტის გამოყენებაზე. ზოგიერთი ვარიანტი მოიცავს თქვენი საკუთარი დაშიფვრის გასაღების დამატებას Google Workspace-ში ან Microsoft 365-ში (როგორც ეს აღწერილია ამ სახელმძღვანელოს სექციაში **მონაცემთა უსაფრთხოება**) ან მსხვილი ორგანიზაციებისთვის შექმნილი ელფოსტის ბოლომდე დაშიფრული სერვისების დანერგვას. როგორიცაა **ProtonMail** Business ან **Tutanota** Business.

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

ვის ესაუბრებით თქვენ და თქვენი თანამშრომლები, წევრები და გუნდები, როდის და სად ესაუბრებით მათ, ხშირად შეიძლება ისეთივე სენსიტიური იყოს, როგორც რაზე საუბრობთ. 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

მიუხედავად იმისა, რომ გამჭვირვალობა მიმდინარე საპარლამენტო ოპერაციებში მნიშვნელოვანია, ასევე მნიშვნელოვანია მეტამონაცემებზე არაავტორიზებული წვდომის შეზღუდვა შეტყობინებების შინაარსის დაცვასთან ერთად). ბოლოს და ბოლოს, მეტამონაცემებს შეუძლიათ ჰაკერების, უცხოური მთავრობების, კომპანიების ან სხვებისთვის იმ სენსიტიური ინფორმაციის გამჟღავნება, რაზეც შეიძლება არ გინდათ,რომ ქონდეთ წვდომა. აქ მოცემულია რამდენიმე მაგალითი, თუ როგორ შეიძლება მეტამონაცემების გამჟღანება:

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 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.

რეკომენდებული კომუნიკაციის დაშიფვრის ინსტრუმენტები თავიდან ბოლომდე

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** • **Tresorit**

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.

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, თქვენ უნდა იცოდეთ რა რისკები არსებობს (ასეთის არსებობის შემთხვევაში), თუ გარკვეულ მეტოქეებს შეუძლიათ გაარკვიონ, ვის ესაუბრებით, როდის ესაუბრებით და (ელფოსტის შემთხვევაში) თქვენი საპარლამენტო შეტყობინებების ზოგადი თემები.

ერთ-ერთი მიზეზი, რის გამოც ასე გულდასმით გირჩევთ **Signal** 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.

ეს შეიძლება არ იყოს კრიტიკული საპარლამენტო კომუნიკაციების უმეტესობისთვის, მაგრამ მნიშვნელოვანია იცოდეთ მეტამონაცემებთან დაკავშირებული რისკები და შესაბამისად აირჩიოთ შესაბამისი საკომუნიკაციო ინსტრუმენტები და პოლიტიკა.

შეგვიძლია ბოლომდე ვენდოთ WHATSAPP-ს?

WhatsApp-ი წარმოადგენს პოპულარულ არჩევანს უსაფრთხო მესინჯერისათვის და შესაძლოა კარგი არჩევანი 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 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 პარლამენტარები და ამომრჩევლები კომუნიკაციისთვის იყენებენ სხვა აპებსა და შეტყობინებების სისტემებს – როგორ დავარწმუნოთ ისინი, რომ ჩამოტვირთონ ახალი აპლიკაცია ჩვენთან კომუნიკაციისთვის?

ხანდახან ადგილი აქვს არჩევანს უსაფრთხოებას და კომფორტს შორის, თუმცა, მცირედ მეტი ძალისხმევა ღირს სენსიტიური კომუნიკაციის დასაცავად. მიეცით კარგი მაგალითი თქვენი კონტაქტებით, იქნება ეს სხვა სამთავრობო უწყებები, ინსტიტუტები, პარლამენტი თუ გარე საარჩევნო ოლქები. თუ იძულებული ხართ გამოიყენოთ სხვა ნაკლებად უსაფრთხო სისტემები, კარგად გაიაზრეთ თუ რას ამბობთ. მოერიდეთ სენსიტიურ თემებზე დისკუსიას. ზოგიერთ პარლამენტს შეიძლება ჰქონდეს განსხვავებული პროტოკოლები ზოგადი ჩეთის ან საჯარო კომუნიკაციისთვის, მაგალითად, ხელმძღვანელობასთან კონფიდენციალური დისკუსიებისთვის. მოახდინეთ თქვენი საპარლამენტო კომუნიკაციების კლასიფიკაცია (შიდა და გარე) კონფიდენციალურობის საფუძველზე და დარწმუნდით, რომ წევრები და თანამშრომლები იყენებენ კომუნიკაციის შესაბამის მექანიზმებს! 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.

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

დისტანციური მუშაობის მიდგომის გაზრდით, დეპუტატებისთვის მნიშვნელოვანია გქონდეთ უსაფრთხო ვარიანტი დიდი ჯგუფური ვიდეო ზარებისთვის ოფისში ან ვირტუალურ ქალაქებში. 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.

პლენარული და კომიტეტის შეხვედრების სპეციფიკური საჭიროებები მოგვიანებით იქნება განხილული ამ სახელმძღვანელოში, მაგრამ თქვენი სხვა უფრო ზოგადი შეხვედრებისთვის, რომლებიც არ საჭიროებენ თანამშრომლობის ფუნქციებს, როგორიცაა ეკრანის გაზიარება ან ოთახებში განაწილება, არსებობს რამდენიმე ვარიანტი. რვა კაციანი ჯგუფისთვის, Signal უაღრესად რეკომენდირებულია. შეგიძლიათ შეუერთდეთ Signal-ის ჯგუფურ ვიდეოზარებს თქვენი სმარტფონიდან ან თქვენი კომპიუტერის Signal დესკტოპის აპიდან. თუმცა, გახსოვდეთ, რომ Signal-ის ჯგუფში შესაძლოა მხოლოდ Signal-ის უკვე მომხმარებელი თქვენი კონტაქტების დამატება.

თუ ეძებთ სხვა ოფციებს, ერთი პლატფორმა, რომელმაც ახლახანს დაამატა აბონენტური დაშიფვრის პარამეტრი, არის **Jitsi Meet**. 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 ან Zoom 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.
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 ღრუბელზე ჩაწერას. Jitsi Meet-ში ჯგუფური დისკუსიის ოთახებს შეუძლია გამორთოს აბონენტური დაშიფვრის ფუნქცია, რაც იწვევს უსაფრთხოების უნებლიე შესუსტებას.

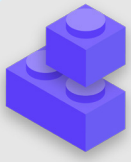
შენიშვნა ფაილების გაზიარების შესახებ

გარდა შეტყობინებების უსაფრთხო გაზიარებისა, ფაილების უსაფრთხო გაზიარება სავარაუდოდ წარმოადგენს თქვენი ორგანიზაციის უსაფრთხოების გეგმის მნიშვნელოვან ნაწილს. ფაილების გაზიარების ოფციების უმეტესობა ჩაშენებულია 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 აუცილებლად 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. პარლამენტში ისეთი მოწყობილობების გამოყენება, როგორიცაა USB, მნიშვნელოვნად ზრდის მავნე პროგრამების ან ქურდობის ალბათობას, ხოლო ელფოსტის ან დანართების სხვა ფორმით გამოყენება ასუსტებს ფიშინგის შეტევებისგან თქვენი პარლამენტის დაცვას.

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:

ელფოსტა	• **Gmail-ი (Google Workspace-ით)** • **Outlook-ი (Office 365-ით)** • არ გამოიყენოთ Microsoft Exchange სერვერი პარლამენტის ელფოსტის სერვისისთვის. თუ ახლა ასრულებთ ამ როლს, უნდა **გადახვიდეთ** Office 365-ზე.
ტექსტური მესინჯერი (ინდივიდუალური ან ჯგუფური)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line-ი** • **KaKao Talk** • **Telegram**
ჯგუფური კონფერენციები, აუდიო და ვიდეო ზარები	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
ფაილების გაზიარება	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**



მონაცემთა უსაფრთხო გადაცემა

- **შეტყობინებების კლასიფიკაცია მათი სენსიტიურობის გათვალისწინებით.**
  - კომუნიკაციისთვის განსაზღვრეთ შესაბამისი სისტემები და ინსტრუმენტები.
  - ჩამოაყალიბეთ პოლიტიკა იმის შესახებ, თუ რამდენ ხანს შეინახავთ შეტყობინებებს, გაითვალისწინეთ როგორც უსაფრთხოება, ასევე პარლამენტის გამჭვირვალობის ვალდებულება.
- **მოითხოვეთ პარლამენტის სენსიტიური შეტყობინებების სანდო გზავნილებისთვის თავიდან ბოლომდე დაშიფვრის სერვისების გამოყენება.**
  - დაუთმეთ დრო პერსონალის და პარტნიორებისათვის იმის განმარტებას, თუ რატომაა უსაფრთხო კომუნიკაცია ამდენად მნიშვნელოვანი; ეს უზრუნველყოფს თქვენი გეგმის წარმატებას.
- **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.
- **ნუ ეცდებით ელფოსტის სერვერის საკუთარი ჰოსტის აწყობას - გამოიყენეთ ღრუბლოვანი ფოსტის სერვისები, როგორიცაა Office 365 ან Google Workspace, როგორც ალტერნატივა.**
  - ნუ მისცემთ საშუალებას პერსონალს გამოიყენოს ელ-ფოსტის პირადი პროფილები სამსახურისათვის.
- **ხშირად შეახსენეთ თანამშრომლებს და წევრებს უსაფრთხოების საუკეთესო პრაქტიკის შესახებ, რომელიც დაკავშირებულია ჯგუფურ შეტყობინებებთან და მეტამონაცემებთან.**
  - იცოდეთ ვინ არის ჩართული ჯგუფურ შეტყობინებებში, ჩეთებში და ელ-ფოსტით მიმოწერაში.

ციფრული პარლამენტები (ელექტრონული პარლამენტი)

როგორც პარლამენტარი, მნიშვნელოვანია განსაკუთრებული ყურადღება მიაქციოთ თქვენი ყველაზე კრიტიკული ფუნქციების კომუნიკაციისა და ოპერატიული უსაფრთხოების პოლიტიკას, მათ შორის, ონლაინ და ციფრულ სივრცეში.

განიხილავს თუ არა თქვენი პარლამენტი სრულ „ელექტრონული პარლამენტის“ სისტემას, რომელსაც შეუძლია ყველაფრის დიგიტალიზაცია მოახდინოს კანონპროექტის შემუშავების, დებატების და ელექტრონულად ხმის მიცემის ჩათვლით (მაგ. Nextsense, Propylon ან Granicus რამდენიმე მაგალითიაა დასახელებული), ან იყენებთ უფრო მარტივ და ნაკლებად ძვირადღირებულ ინსტრუმენტებს თქვენი საპარლამენტო მუშაობის გასაადვილებლად, მნიშვნელოვანია განიხილოთ, თუ როგორ ითვალისწინებს ნებისმიერი ინსტრუმენტი (ან ინსტრუმენტები) და პროცესი (ან პროცესები) უსაფრთხოების, მთლიანობასა და ხელმისაწვდომობას.

უსაფრთხოება და ციფრული პარლამენტები

როგორც ვნახეთ ინციდენტების სერია სამხრეთ აფრიკაში, საპარლამენტო ოპერაციების ციფრულ სამყაროზე გადასვლა მოითხოვს განსაკუთრებულ ყურადღებას კიბერუსაფრთხოების კუთხით, რათა თავიდან იქნას აცილებული არა მხოლოდ სენსიტიური მონაცემების დაკარგვა ან ქურდობა, არამედ უხერხულობის, დამცირების შესაძლებლობა და წევრებისა და პერსონალისთვის ზიანი მიყენება. 2020 წლის მაისში პორნოგრაფიული სურათები გამოჩნდა ქვეყნის ეროვნული ასამბლეის ვირტუალური შეხვედრის დაწყებამდე რამდენიმე წუთით ადრე. შეურაცხმყოფელი სურათების ჩვენების შემდეგ, „ჰაკერმა“ ან „ზუმ-ბომბერმა“ შემდეგ სექსისტური და რასობრივი შეურაცხყოფა მიაყენა სხდომის სპიკერს, რომელიც ხელმძღვანელობდა შეხვედრას, რითაც აიძულა შეხვედრა გადაედო. მსგავსი ინციდენტი ასევე ერთი თვით ადრე მოხდა, როცა ქალთა, ახალგაზრდობისა და შშმ პირთა მინისტრის ხელმძღვანელობით მიმდინარეობდა შეხვედრა და პორნოგრაფიული სურათების ჩვენების გამო ჩაშალა.

დისტანციური პლენარული და კომიტეტის სხდომები

ამ პროცესებს შორის მთავარია პლენარული და კომიტეტის სხდომები. ეს შეხვედრები და მათში ჩატარებული საუბრები, გადაწყვეტილებები და კენჭისყრა უდევს საფუძვლად თქვენი პარლამენტის მუშაობის დიდ ნაწილს და, როგორც ასეთი, შეიძლება მეტოქესთვის კონკრეტულ სამიზნეს წამოადგენდეს დღევანდელ პანდემიით დაზარალებულ სამყაროში, ეს სესიები და შეხვედრები იმართება სულ უფრო მრავალფეროვანი ფორმით, თქვენი ქვეყნის კონტექსტიდან გამომდინარე, როგორც პირადად, მთლიანად ონლაინ და „ჰიბრიდული“ ფორმით.

როგორც აღნიშნულია წარმომადგენელთა პალატის მიერ გამოცემული ბოლო სახელმძღვანელოში **პარლამენტები, რომლებიც რეაგირებენ პანდემიაზე**, საპარლამენტო დებატების ტიპიური სტრუქტურა განსხვავდება ტიპიური საკონფერენციო დისკუსიისგან ან სტანდარტული ორგანიზაციული შეხვედრისგან. დისტანციური კენჭისყრის საჭიროება, ფორმალური წინადადებებისა და ცვლილებების წარდგენა, სტრუქტურირებული დებატები და თუნდაც ერთდროული თარგმანი ყველა ამომრჩევლის მონაწილეობის უზრუნველსაყოფად, ხშირად მოითხოვს დამატებით ფუნქციებს, რომლებიც არ მოიძებნება სტანდარტული ტექნოლოგიური გადაწყვეტილებების უმეტესობაში. შედეგად, ვირტუალური ან ჰიბრიდული სესიის მასპინძლობისას, თქვენს პარლამენტს სავარაუდოდ დასჭირდება შეიმუშაოს (ან უკვე შეიმუშავა) მორგებული პროგრამული უზრუნველყოფა ან შეიძინოს ძვირადღირებული გადაწყვეტილებები (მაგ. **Cisco-ს Webex Legislate**). შექმნილია სპეციალურად პარლამენტის სესიების დისტანციურად სამართავად. რომელ ვარიანტსაც აირჩევს თქვენი პარლამენტი, იმის მიხედვით მნიშვნელოვანია მან განიხილოს, როგორც ეს მოცემულია სახელმძღვანელოში **პარლამენტის პასუხი პანდემიაზე**, როგორ შეძლებს ყველა წევრი და თანამშრომლეი წვდომას ასეთ სისტემაზე. ასევე ძალიან მნიშვნელოვანია იმის უზრუნველყოფა, რომ ასეთი სისტემა ადეკვატურად იყოს დაცული.

პარლამენტის სესიებისთვის ტექნიკური გადაწყვეტილებების შემუშავებისა და გამოყენების დროს მნიშვნელოვანია უსაფრთხოების ძირითადი საფუძვლების უზრუნველყოფა. ეს მოიცავს ნაბიჯებს იმის უზრუნველსაყოფად, რომ პასიურ რეჟიმში მონაცემები დაცული იყოს თავად სისტემაში, რომ ისინი სათანადოდ დაშიფრული იყოს გადაცემის დროს და მხოლოდ ავტორიზებულ მომხმარებლებს შეეძლოთ სისტემაზე წვდომა. არსებობს მრავალი მიდგომა, რომელიც შეიძლება გამოყენებული იქნას ასეთი უსაფრთხოების მისაღწევად, მათ შორის ბევრი ძირითადი პრინციპი, რომლებიც აღწერილია ამ სახელმძღვანელოს დანარჩენ ნაწილში. მონაცემთა და კომუნიკაციის ნებისმიერ სისტემაში თავიდან ბოლომდე დაშიფვრა, ძლიერი პაროლის და ორფაქტორიანი ავთენტიფიკაციის მოთხოვნები და/ან ასეთ სისტემებზე მომხმარებლის IP მისამართით წვდომის შეზღუდვა (თუ ისინი საჯარო წვდომისთვის არ არის განკუთვნილი), ვირტუალური კერძო ქსელების მოთხოვნა (რაც შემდგომში იქნება განხილული სახელმძღვანელოში) და მხოლოდ სანდო, ვისურსებისგან სუფთა მოწყობილობებზე შეზღუდული წვდომა ყველაზე მისაღები ნაბიჯებია ასეთ დროს.

დისტანციურად ხმის მიცემა

ძლიერი უსაფრთხოება, ალბათ, ყველაზე მნიშვნელოვანია დისტანციური ხმის მიცემის დროს. როგორც ზემოხსენებულ **პარლამენტები, რომლებიც რეაგირებენ პანდემიაზე** სახელმძღვანელოშია ნათქვამი, დეპუტატები აირჩევიან პარლამენტში მათი ამომრჩევლების სახელით კონკრეტული მიზნით კენჭისყრაში მონაწილეობის მისაღებად. ამ ხმების ნდობისა და გადამოწმების შესაძლებლობა გადამწყვეტია არა მხოლოდ თქვენი პარლამენტის ფუნქციონირებისთვის, არამედ მთლიანად დემოკრატიული სისტემისთვის. ასეთი ხმების გადამოწმება შედარებით ადვილია, როდესაც პარლამენტის წევრი კენჭისყრაში მონაწილეობს პირადად, მაგრამ ვირტუალური მონაწილეობით ტექნიკური ავთენტიფიკაცია უფრო რთული ხდება, რაც დიდ ზრუნვას და ყურადღებას მოითხოვს. როგორც ნათქვამია კანადის თემთა პალატის წარმომადგენელთა პალატის პროცედურებისა და ბიზნესის მუდმივმოქმედი კომიტეტისთვის მიცემული ექსპერტის **ჩვენებაში**, პარლამენტები ჩვეულებრივ ირჩევენ დისტანციური ხმის მიცემის ოთხი ვარიანტიდან ერთ-ერთს:

- ელექტრონული ფოსტით ხმის მიცემა: მონაწილეები იღებენ ხმის მიცემის ელექტრონულ ფორმას და აგზავნიან თავიანთ ხმას ელექტრონული ფოსტით. ეს ვარიანტი ზოგადად დაუცველად ითვლება, ნაწილობრივ ბოლომდე დაშიფვრის არარსებობის გამო და თავიდან უნდა იქნას აცილებული.
- ონლაინ ხმის მიცემა: როდესაც წევრებს წვდომა აქვთ და ხმის მიცემის უფლებას აძლევენ მათ ვებსაიტზე კომპიუტერით ან მობილური ტელეფონით. ეს მიდგომა მოითხოვს უსაფრთხო ინფრასტრუქტურაში ინვესტიციას, მათ შორის უსაფრთხო მოწყობილობებს ძლიერი ავთენტიფიკაციით, როგორც ზემოთ იქნა აღნიშნული.
- აპზე დაფუძნებული ხმის მიცემა: როდესაც წევრები ჩამოტვირთავენ წვდომის მისაღებად და ხმის მისაცემად აპლიკაციას. აღნიშნული ინტერნეტით ხმის მიცემის მსგავსია, მაგრამ იყენებს სპეციალურ აპლიკაციას, რომლის ჩამოტვირთვა შესაძლებელია ტელეფონში ან ტაბლეტში და წვდომა ხორციელდება ბრაუზერის საშუალებით.
- ვიდეო ხმის მიცემა: მონაწილეები ხმას აძლევენ ეკრანზე ხელის აწევით ან ხმოვანი ხმის მიცემით. არაანონიმური ხმის მიცემის შემთხვევაში, ეს შეიძლება იყოს ტექნიკურად ყველაზე ნაკლებად რთული და ტექნიკურად ყველაზე ნაკლებად გასამართი და უსაფრთხო. თუმცა, ეს მაინც მოითხოვს ძლიერ დაშიფვრას და ავთენტიფიკაციის სისტემებს, რათა თავიდან იქნას აცილებული პიროვნების გარეგნობის გაყალბება ან შეფერხება ხმის მიცემის დროს.

დისტანციური კენჭისყრის რომელი ვარიანტიც არ უნდა აირჩიოს თქვენმა პარლამენტმა – თუ ის საერთოდ გამოიყენებს დისტანციურ კენჭისყრას – მნიშვნელოვანია, მხედველობაში იქონიოთ კიბერუსაფრთხოების საფუძვლები მთელი ხმის მიცემის პროცესში. ასეთი ძირითადი პრინციპები მოიცავს იმის უზრუნველყოფას, რომ მოწყობილობები, რომლებსაც დეპუტატები ხმის მისაცემად იყენებენ იყოს ფიზიკურად და მავნე პროგრამებისგან დაცული, რომ დეპუტატების ინტერნეტთან წვდომა სათანადოდ იყოს დაცული კენჭისყრის დროს

(ისევე, როგორც სხვა საპარლამენტო საქმიანობის შემთხვევაში) და დეპუტატებს ჰქონდეთ სტაბილური ინტერნეტი კავშირი იმისთვის, რომშეძლონ ხმის მიცემა საჭიროების შემთხვევაში. როგორც ასახულია პარლამენტები, რომლებიც რეაგირებენ პანდემიაზე სახელმძღვანელოში, დისტანციურ კენჭისყრაზე გადასვლისას სისტემა საფუძვლიანად უნდა შემოწმდეს, სანამ ის გააქტიურდება, ხოლო დეპუტატებს უნდა ჰქონდეთ მხარდაჭერა და ტრენინგი გავლილი სისტემის ეფექტურად გამოყენების მიზნით. მნიშვნელოვანია გვახსოვდეს, რომ უსაფრთხოების ნაწილია *ხელმისაწვდომობა*. ასევე აუცილებელია უზრუნველყოფილი იქნასრომ დეპუტატ ქალებსა და თანამშრომლებს შეეძლოთ უსაფრთხოდ გამოიყენონ ონლაინ სისტემები, მათ შორის დისტანციური კენჭისყრის სისტემა და ამისთვის ჰქონდეთ წვდომა ტექნოლოგიებზე. როდესაც ქალები, განსაკუთრებით არჩეული ქალები, შედიან ინტერნეტში, ისინი აწყდებიან დაშინებისა და შევიწროების უფრო მაღალ დონეს და ეს ფაქტორი მხედველობაში უნდა იქნას მიღებული ისეთი ტექნოლოგიების შემუშავებისა და გამოყენების დროს, როგორიცაა დისტანციური ხმის მიცემა, რათა ყველა დეპუტატს შეეძლოს თავისი ფუნქციების ეფექტურად შესრულება. გარდა ამისა, ძალზე მნიშვნელოვანია სათანადო დისტანციური მრავალენოვანი წვდომის უზრუნველყოფა იმ ქვეყნებში, სადაც წევრები და თანამშრომლები საუბრობენ რამდენიმე ოფიციალურ ენაზე.

ელპარლამენტის პროვაიდერი და პროგრამული უზრუნველყოფის უსაფრთხოება

ნებისმიერი პროგრამული უზრუნველყოფა - რომელიც გამოყენებული იქნება დისტანციური კენჭისყრისთვის თუ უფრო ფართო საპარლამენტო მიზნებისთვის- **უნდა იყოს თქვენს მიერ შეძენილი დაცული და აკრედიტებული წყაროდან, უსაფრთხოების ტესტირება ჩატარებული უნდა იყოს დამოუკიდებელი ჯგუფების მიერ და იყოს სერტიფიცირებული.** მნიშვნელოვანია გვახსოვდეს, რომ პროგრამული უზრუნველყოფის დეველოპერები, რომლებსაც თქვენ დაქირავებთ აპლიკაციის ან ინსტუმენტების შესაქმნელად, სულაც არ არიან უსაფრთხოების ექსპერტები. როგორც ასეთი, უსაფრთხოების ექსპერტების ჩართვა აუდიტის საშუალებით თქვენი განაცხადის შესამოწმებლად უსაფრთხოების პოტენციური ხვრელებისთვის, მნიშვნელოვანია თქვენი პლატფორმის, ინტრუმენტის ან აპლიკაციის გატეხვის ან შეღწევის რისკის შესამცირებლად. პროგრამის საუკეთესო დეველოპერებსაც კი შეიძლება შეცდომები გაეპაროს ექსპერტთა მეორე (ან მესამე) ჯგუფის მიერ მუშაობის შემოწმების გარეშე!

დისტანციური ხმის მიცემა რეალურ სამყაროში

სხვადასხვა პარლამენტმა დანერგა დისტანციური ხმის მიცემის სისტემები და ამით გადადგა მნიშვნელოვანი ნაბიჯები წევრთა ხმების უსაფრთხოებისა და მთლიანობის უზრუნველსაყოფად. ამ პროცესის ერთ-ერთი ელემენტი, როგორც ეს ზემოთ ავღნიშნეთ,არის სათანადო ავთენტიფიკაციის უზრუნველყოფა. რამდენიმე მაგალითი მოცემულია გაერთიანებული სამეფოდან. თემთა პალატა, სადაც წევრები კენჭისყრისთვის თავიანთ საპარლამენტო ანგარიშებში შესასვლელად იყენებენ ერთჯერადი სისტემაში შესვლის პროცესს, რაც მოითხოვს პაროლის გამოყენებას კონკრეტულ, სახელობით მოწყობილობაზე. ესპანეთში დეპუტატებს ენიჭებათ პერსონალური კოდები, რომლებიც უნდა შეიყვანონ სმარტფონის აპის მეშვეობით, სანამ ხმის მიცემა დისტანციურად მოხდება. ჩილეში სენატორები, რომლებიც ხმას დისტანციურად აძლევენ საგულდაგულოდ შემუშავებულ დისტანციური ხმის მიცემის აპლიკაციის გამოყენებით, უნდა ჩანდნენ ეკრანზე, იმისთვის, რომ ხმის მიცემა შეძლონ.

მონაცემების უსაფრთხოდ შენახვა

პარლამენტების უმრავლოსობისთვის ერთ-ერთი ყველაზე მნიშვნელოვანი გადაწყვეტილებაა სად შეინახონ 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 ღრუბლოვან საცავებში. ალბათ ყველაზე ტიპური მაგალითები მოიცავს Microsoft 365-ს და Google Drive-ს. ღრუბლოვანი საცავის ყოვლისმომცველი გეგმის გარეშე სავარაუდოა, რომ თქვენი პარლამენტის მონაცემები ინახება სხვადასხვა ადგილებში - მათ შორის, თანამშრომლების 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.

მონაცემთა შენახვა და პარლამენტები

ხელმისაწვდომი (ზოგჯერ უფასო) ღრუბლოვანი საცავის გამოჩენამ მრავალ პარლამენტსა და სხვა ორგანიზაციებს ცხოვრება გაუმარტივა (და უსაფრთხო გახადა). 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. შეტევის დროს გატეხეს ლოკალური სერვერები, მათ შორის ნორვეგიის პარლამენტის სერვერი, რამაც ჰაკერებს საშუალება მისცა წვდომა ჰქონოდათ საპარლამენტო ელფოსტის ანგარიშებზე, დაეყენებინათ დამატებითი მავნე პროგრამა მსხვერპლის სერვერებზე და დაკავშირებულ სისტემებზე და შეუზღუდავად წაეღოთ [სენსიტიური მონაცემები](). ჰაკერობის გასაჯაროების შემდეგ, სანამ Microsoft 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 პარლამენტებისთვის და სხვა ორგანიზაციებისათვის, რომლებიც თავად ასრულებენ ჰოსტის როლს საკუთარი ელფოსტის სერვერებისა და სხვა ტიპის სენსიტიური მონაცემებისთვის კიბერუსაფრთხოების პერსონალში.

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 პარლამენტის ადგილობრივი სერვერი. მათთვის გაცილებით რთულია გატეხონ Google-ის ან Microsoft-ის უსაფრთხოების დაცვის სისტემები. კარგ ქლაუდ-საცავ კომპანიებს გააჩნია შეუდარებელი უსაფრთხოების რესურსები და ურყევი ბიზნეს-სტიმული უზრუნველყოს საკუთარი მომხმარებლის უსაფრთხოება. მოკლედ: სანდო ქლაუდ-საცავის სტრატეგია გაცილებით მარტივია სარეალიზაციოდ და უსაფრთხოების დასაცავად დროის ხანგრძლივი პერიოდის განმავლობაში. ასე რომ, იმის ნაცვლად, რომ დაადგინოთ (და შეინახოთ) კიბერუსაფრთხოების ერთგული და მაღალკვალიფიციური პერსონალის რაოდენობა, რომელიც საჭიროა თქვენი პარლამენტის ადგილობრივი სერვერების დასაცავად, თქვენი ენერგია მიმართეთ რამდენიმე მარტივ ამოცანაზე. ეს მოიცავს ღრუბლოვანი საცავის სწორი ვარიანტის არჩევას თქვენი მონაცემების კონფიდენციალურობისა და ლოკალიზაციის საჭიროებებისთვის, ანგარიშის ძლიერი უსაფრთხოების შენარჩუნებას, პერსონალის სწავლებას, თუ როგორ სწორად გააზიარონ (და არ გააზიარონ) საქაღალდეები და დოკუმენტები (ზოგადად, თქვენ უნდა იქონიოთ საქაღალდეები ღრუბლოვან საცავის დისკზე, რომელიც უშვებს წვდომას მხოლოდ იმ თანამშრომლებზე, რომლებსაც სჭირდებათ ეს გარკვეული ფაილები) და რეგულარულად ამოწმოთ თქვენი სისტემა, რათა დარწმუნდეთ, რომ თანამშრომლები და წევრები არ „აზიარებენ" ფაილებს (მაგალითად, ფაილებისთვის არ აქვთ ჩართული უნივერსალური გაზიარების ბმული, რომელიც სინამდვილეში განსაზღვრულია მხოლოდ რამდენიმე ადამიანისთვის). 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? აუცილებელია თუ არა თავად წევრის კუთვნილი მონაცემების გამიჯვნა იმ ინფორმაციისგან, რომელიც თავად პარლამენტი ამუშავებს? 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.

შეგვიძლია ნამდვილად ვენდოთ ღრუბლოვან საცავს?

მოკლედ, ღრუბლოვან საცავშიინფორმაციის შენახვაში არსებითად მიუღებელი არაფერია. როგორც ზემოთ ავღნიშნეთ, ღრუბლოვანი საცავის მსხვილ პროვაიდერებს ჰყავთ მსოფლიოს საუკეთესო უსაფრთხოების ინჟინრების გუნდები, რომლებიც ყოველდღიურად მუშაობენ თავიანთი პროდუქციის უზრუნველსაყოფად და მომხმარებლებს სთავაზობენ უსაფრთხოების მხარდაჭერას იმაზე მეტს რაც ყველაზე მცირე IT დეპარტამენტებს შეუძლიათ დამოუკიდებლად უზრუნველყონ. თუმცა, გახსოვდეთ, რომ ღრუბლოვანი საცავის ტრადიციული სერვისები, როგორც წესი, მოითხოვს სენსიტიურ მონაცემებზე წვდომის მიწოდებას მომსახურების მესამე მხარის პროვაიდერისთვის. **აღნიშნულთან ერთად, თითოეულ ცალკეულ პარლამენტს ექნება საკუთარი პოლიტიკური მოსაზრებები და სამართლებრივი მოთხოვნები (როგორიცაა მონაცემთა ლოკალიზაციის მანდატები), რომლებიც უნდა მხედველობაშ იქნეს მიღებული, როდესაც არჩევს, შეუძლია თუ არა მას ენდოს და გამოიყენოს ღრუბლოვანი საცავის კონკრეტული პროვაიდერი.**

ქლაუდ-საცავის რომელი პროვაიდერი უნდა ავირჩიოთ?

თუ თქვენს პარლამენტს არ უწევს მონაცემთა ლოკალიზაციის მოთხოვნების გათვალისწინება და არ აქვს პრობლემები სანდო მესამე მხარესთან, რომელიც უზრუნველყოფს მონაცემებზე წვდომას, ღრუბლოვანი საცავის ორი ყველაზე პოპულარული ვარიანტია Google Workspace (ადრე ცნობილი როგორც GSuite) და Microsoft 365. თუ თქვენი პარლამენტი უკვე იყენებს Gmail-ს, Google Workspace-ში დარეგისტრირება და მონაცემების Google Drive-ში შენახვა მისი ჩაშენებული Google Docs, Sheets და Slides აპებით სიტყვების დამუშავებისთვის, ელცხრილებისა და პრეზენტაციებისთვის ძალიან ლოგიკურია. ანალოგიურად, თუ თქვენი პარლამენტი იყენებს Excel-სა და Word-ს, უმარტივესი გზაა დარეგისტრირდეთ Microsoft 365-ზე, რომელიც გაძლევთ წვდომას Outlook-ზე ელფოსტისთვის და Microsoft Word-ის, Excel-ის, PowerPoint-ისა და Teams-ის ლიცენზირებულ ვერსიებს.

რა მოხდება, თუ ჩვენ გვჭირდება საკუთარი მონაცემების კონტროლი ან მონაცემთა ლოკალიზაციის კანონების დაცვა?

ბევრი პარლამენტისთვის ეს მარტივი ვარიანტი შეიძლება არ იყოს მისაღები მონაცემთა ლოკალიზაციის მოთხოვნების ან კონკრეტული მოლოდინების გათვალისწინებით, რომლებიც მოითხოვს ექსკლუზიურ საპარლამენტო კონტროლს საკუთარ მონაცემებზე. კარგი ამბავი ის არის, რომ უსაფრთხო ღრუბლოვანი საცავის პროვაიდერებმა ახლახან შეიმუშავეს ვარიანტები, რომლებიც საშუალებას აძლევს მომხმარებლებს ან აირჩიონ თავიანთი მონაცემების მდებარეობა (გაითვალისწინეთ, რომ ეს მოცემულ მომენტში განკუთვნილია მხოლოდ ევროპელი მომხმარებლებისთვის) ან გააკონტროლონ საკუთარი შიფრაციის გასაღებები. **პრაქტიკაში ეს ნიშნავს, რომ თქვენს პარლამენტს აქვს შესაძლებლობა მართოს საკუთარი მონაცემები, მაგრამ ამავე დროს ისარგებლოს ღრუბლოვანი საცავის ინფრასტრუქტურითა და უსაფრთხოებით.**

თუ თქვენი პარლამენტი ამჟამად იყენებს ან დაინტერესებულია Google Workspace-ით მონაცემთა ღრუბლოვანი შენახვით და გაზიარებით, Google-მა შემოიღო ფუნქცია, რომელიც იძლევა **კლიენტის მხრიდან დაშიფვრის შესაძლებლობას** Enterprise Plus ტიპის ორგანიზაციებისთვის. მიუხედავად იმისა, რომ ეს ფუნქცია ამჟამად ტესტირების პროცესშია და ხელმისაწვდომია მხოლოდ Google Workspace-ის ყველაზე ძვირადღირებულ გეგმებზე, ის საშუალებას გაძლევთ ისარგებლოთ Google Drive-ის შენახვისა და გაზიარების ფუნქციებითა და მათი ჩაშენებული უსაფრთხოების ფუნქციებით, ასევე შეზღუდოთ d Google-ით წვდომა თქვენი პარლამენტის კონფიდენციალურ ან პირად ინფორმაციაზე. კლიენტის მხარის დაშიფვრით, შეგიძლიათ გააერთიანოთ გასაღების მართვის დამატებითი სერვისი, როგორიცაა Virtru და საშუალება მისცეთ მომხმარებლებს მართონ საკუთარი დაშიფვრის გასაღებები თავად Google-ზე წვდომის გარეშე. ასეთი სერვისი მოითხოვს, რომ ყველამ დიდი სიფრთხილე გამოიჩინოს ამ გასაღებების დაცვაში, რათა სათანადოდ უზრუნველყოს წვდომა გასაღების მართვის ნებისმიერ სისტემაზე, რომლის ინტეგრირებასაც Google Workspace-თან გადაწყვეტთ. ანგარიშის ადმინისტრატორებს შეუძლიათ შეიტყონ მეტი, თუ როგორ უნდა ჩართონ კლიენტის მხრიდან დაშიფვრა Google Workspace-**ის მხარდაჭერის გვერდზე**.

თუ თქვენი პარლამენტი ამჟამად იყენებს ან აინტერესებს Microsoft 365 ღრუბლოვან მონაცემთა შენახვისა და გაზიარებისთვის, ის გთავაზობთ ოდნავ უფრო რთულ, მაგრამ კარგად ჩამოყალიბებულ ვარიანტს საკუთარი დაშიფვრის გასაღებების სამართავად, რომელიც ცნობილია როგორც **Microsoft 365 Double Key Encryption**. უსაფრთხოების ეს პარამეტრი მოითხოვს **Microsoft 365 E5**, მაგრამ გაძლევთ საშუალებას აკონტროლოთ ნებისმიერი სენსიტიური ან პერსონალური საპარლამენტო მონაცემი და შეუზღუდოთ წვდომა თვით Microsoft-საც კი.

Tresorit კიდევ ერთი ვარიანტია, რომლის განხორციელებაც უფრო ადვილია, თუ თქვენი პარლამენტი ფიქრობს, რომ მესამე მხარეს შეიძლება ქონდეს შიდა ინფორმაციაზე წვდომა. Tresorit უზრუნველყოფს თავიდან ბოლომდე დაშიფვრის სერვისს ღრუბლოვანი საცავის და ფაილების გაზიარების შემთხვევაში, ასევე **მონაცემთა შენახვის მრავალფეროვან ვარიანტს**.

რა მოხდება, თუ ჩვენ არ ვენდობითთ ღრუბლოვანი საცავის რაიმე გადაწყვეტილებას?

თუ თქვენ გადაწყვეტთ თავად გაართვათ თავი და დაეყრდნოთ ადგილობრივ სერვერებს თქვენი პარლამენტის მონაცემების შესანახად, აუცილებელია ჩადოთ მნიშვნელოვანი დრო და რესურსები თქვენი პარლამენტის მოწყობილობების ციფრული უსაფრთხოების გასაძლიერებლად და უზრუნველსაყოფად, რომ ასეთი სერვერები სათანადოდ არის კონფიგურირებული, დაშიფრული, და შენახული და ფიზიკურად დაცული. როგორც ზემოთ აღინიშნა, ეს მიდგომა მოითხოვს კიბერუსაფრთხოების ერთგული და მაღალკვალიფიციური პროფესიონალების იდენტიფიცირებას, დაქირავებას და შენარჩუნებას თქვენი შიდა სერვერის ინფრასტრუქტურის უზრუნველსაყოფად.

პარლამენტის ღრუბლოვანი ანგარიშების უსაფრთხოების გაუმჯობესება

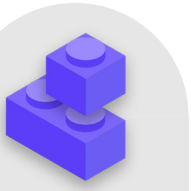
თუ თქვენი პარლამენტი გადაწყვეტს დომენის შექმნას Google Workspace-ში ან Microsoft 365-ში, გაითვალისწინეთ, რომ ორივე კომპანია გთავაზობთ უფრო მაღალ უსაფრთხოებას რისკის ქვეშ მყოფი ანგარიშებისთვის. **Google-ის გაფართოებული დაცვა** და **Microsoft AccountGuard** უზრუნველყოფს კიდევ უფრო უკეთეს დაცვას კვალიფიციური ორგანიზაციების ღრუბლოვანი ანგარიშებისთვის და მნიშვნელოვნად ამცირებს ეფექტური ფიშინგის და ანგარიშის გატეხვის შანსებს. თუ ფიქრობთ, რომ თქვენი პარლამენტი უფლებამოსილია და დაინტერესებულია თქვენი წევრებისა და პერსონალის რომელიმე გეგმაში გაწევრიანებით, გთხოვთ, ეწვიოთ ზემოთ მოცემულ ვებგვერდებს ან დაუკავშირდეთ **cyberhandbook@ndi.org** შემდგომი დახმარების მისაღებად.

მონაცემების დუბლირება

მნიშვნელობა არ აქვს, თქვენი პარლამენტი მონაცემებს ფიზიკურ მოწყობილობებსა და სერვერებზე ინახავს თუ ღრუბელში, მნიშვნელოვანია გქონდეთ სარეზერვო ასლები. 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 მოიპარონ 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 მოიპარონ. 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.

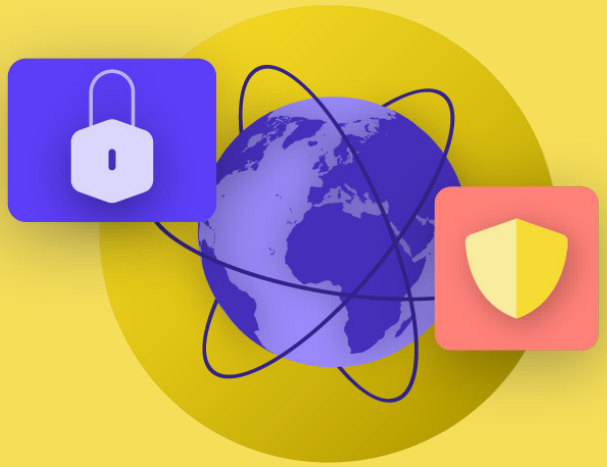
თუ თქვენი პარლამენტი იყენებს ღრუბლოვან-საცავს (როგორიცაა Google Drive-ი), Google-ის წაშლის ან თქვენი მონაცემების ავარიული განადგურების რისკი საკმაოდ დაბალია, თუმცა, ადამიანური შეცდომა (როგორიცაა მნიშვნელოვანი ფაილების შემთხვევით წაშლა) მაინც შესაძლებელია. დაათვალიერეთ ღრუბლოვანი სარეზევო კოპირების გადაწყვეტილება როგორიც არის **Backupify** ან **SpinOne Backup**.

თუ მონაცემები ინახება ადგილობრივ სერვერზე და/ან ადგილობრივ მოწყობილობებში, უსაფრთხო რეზერვი კიდევ უფრო მნიშვნელოვანი ხდება. შეგიძლიათ თქვენი პარლამენტის მონაცემების სარეზერვო კოპირება გარე მყარ დისკზე ან დისკების სერიაზე, მაგრამ დარწმუნდით, რომ ასეთი დისკები დაშიფრულია 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.



მონაცემების უსაფრთხოდ შენახვა

- **შეინახეთ სენსიტიური მონაცემები მხოლოდ სანდო ქლაუდ-საცავის სერვისში.**
  - უზრუნველყავით ნებისმიერ დაკავშირებულ პროფილს, რომელიც გამოიყენება აღნიშნულ სერვისზე წვდომისათვის, გააჩნდეს ძლიერი პაროლი და 2FA-ი.
- **შემოიღეთ და აღასრულეთ პოლიტიკა, რათა შეიზღუდოს გაზიარების პარამეტრები ქლაუდის ფარგლებში.**
  - ასწავლეთ ყველა წევრს და თანამშრომლეს, როგორ გააზიარონ დოკუმენტები სწორად (და არა ხშირად).
- **თუ თქვენს პარლამენტს ურჩევნია მონაცემთა ადგილობრივად შენახვა, ინვესტიცია ჩადეთ კვალიფიციურ IT პერსონალში.**
- **უსაფრთხოდ შეინახეთ თქვენი მონაცემების რეზერვი - დაშიფრეთ სარეზერვო მყარი დისკები ან სხვა სარეზერვო მოწყობილობები.**



უსაფრთხოების დაცვა ინტერნეტში

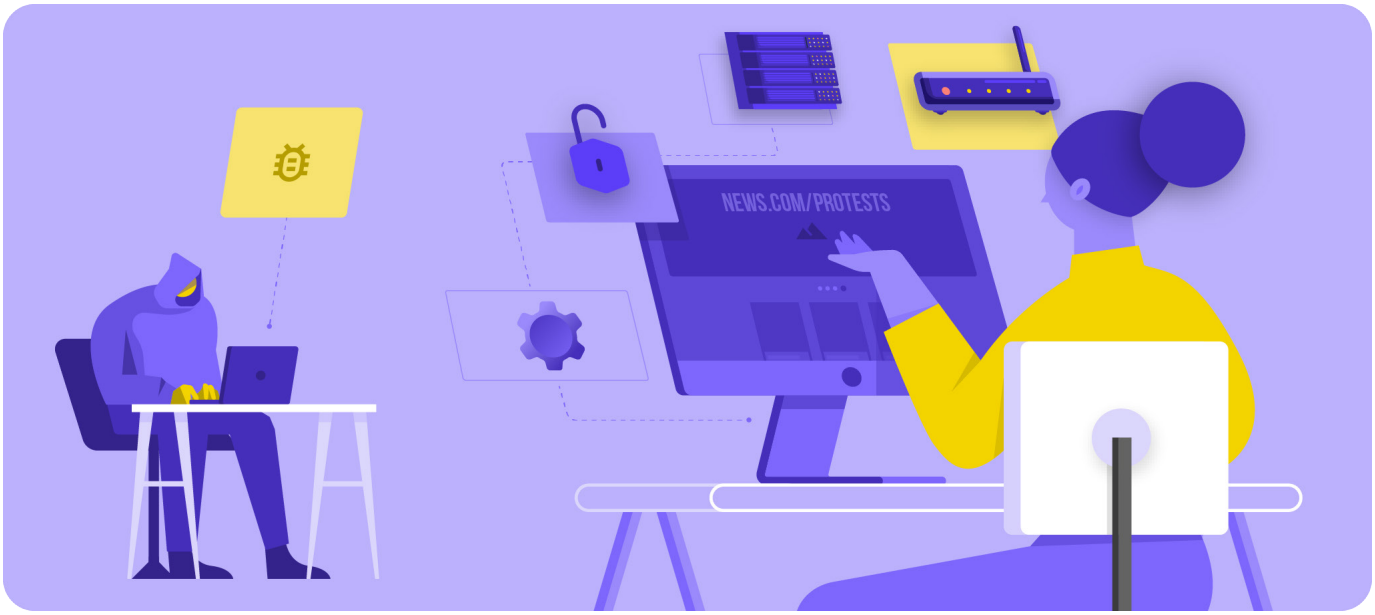
ინტერნეტის თქვენს ტელეფონში ან კომპიუტერში გამოყენების დროს, თქვენს აქტივობას ბევრი რამის თქმა შეუძლია თქვენი და თქვენი ორგანიზაციის შესახებ.

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.



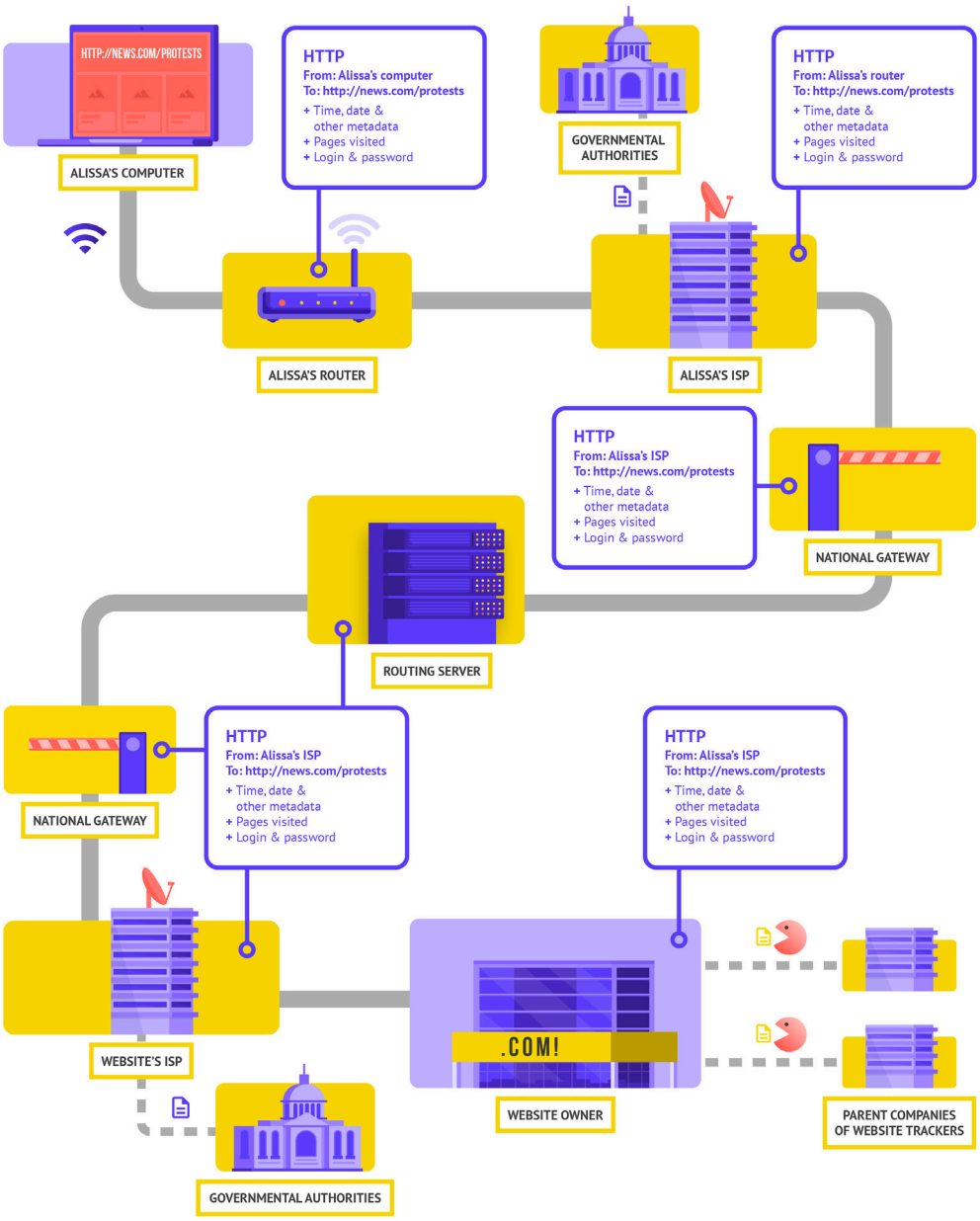
მეთვალყურეობა, ცენზურა და პარლამენტები

სულ უფრო ხშირად იყენებენ სათვალთვალო ტექნოლოგიებს და ზოგიერთ შემთხვევაში უბრალოდ Wi-Fi-ის ჰაკერები, მტრულად განწყობილი მთავრობები და საფრთხის სხვა წყაროები მთელს მსოფლიოში, რათა აკონტროლონ პარლამენტში მომუშავე დეპუტატების და სხვათა ონლაინ აქტივობა. მაგალითად, 2013 წელს ჰაკერებმა მოიპარეს ევროპარლამენტის თანამშრომლებისა და ვიზიტორების მონაცემები **პარლამენტის საჯარო Wi-Fi ქსელში შეღწევის გზით**. ბევრად უფრო დახვეწილი თავდასხმების მოლოდინი მომავალ წლებში.

ინტერნეტ ტრაფიკის დაჭერის და მონაცემების მოპარვის გარდა, თავდამსხმელები ასევე ხელს უშლიან მნიშვნელოვან საპარლამენტო ოპერაციებს ინტერნეტის და სისტემების დაბლოკვით. 2021 წლის მაისში ბრიუსელში ბელგიის პარლამენტმა შეწყვიტა მუშაობა **სერვისზე მასიურად მიუწვდომლობის გამო**. შეტევის გამო გადაიდო ზოგიერთი დებატები და კომიტეტის სხდომები, რადგან მომხმარებლებს არ შეეძლოთ წვდომა ვირტუალურ სერვისებზე, რომლებიც საჭირო იყო სესიაში მონაწილეობის მისაღებად.

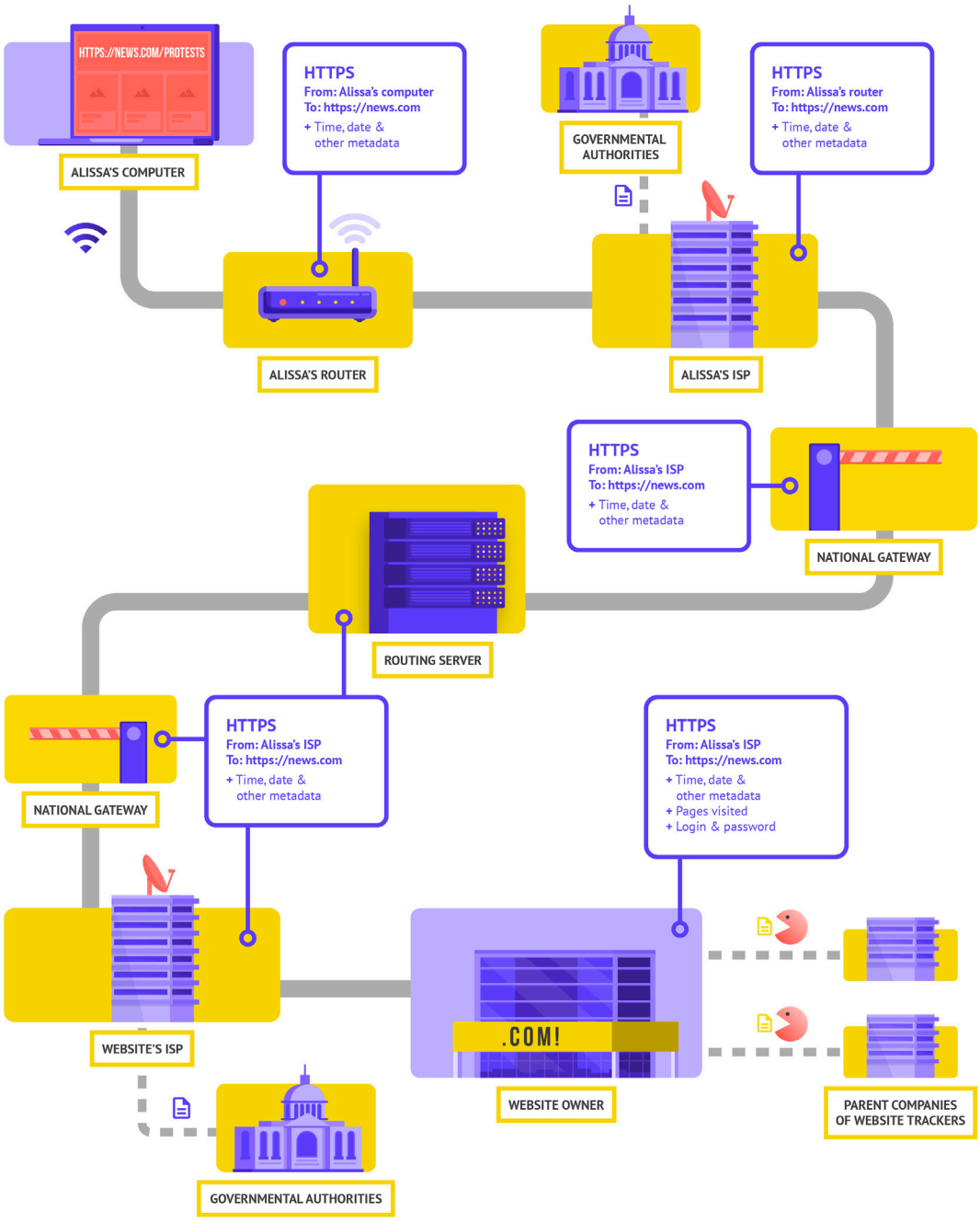
ინფორმაციასთან წვდომაზე და მის ონლაინ თავისუფლებაზე ხსენებული შეტევების მზარდი სიხშირე ხაზს უსვამს რამდენად მნიშვნელოვანია პარლამენტისთვის ესმოდეთ ინტერნეტში მუშაობის რისკი და შეიმუშაონ გეგმები მასზედ, თუ როგორ მოახდინონ დაკავშირება, როცა კავშირი შეფერხებულია.

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



დაშიფვრის გარეშე ბრაუზინგისას დაუცველია ყველა თქვენი მონაცემი. როგორც ზემოთ იყო ნაჩვენები, მეტოქეს შეუძლია დაინახოს სად ხართ, რომ გადადიხართ news.com-ზე, ათვალიერებთ კონკრეტულად გვერდს თქვენს ქვეყანაში მიმდინარე საპროტესტო აქციების შესახებ და, რაც ყველაზე მნიშვნელოვანია, როგორც დეპუტატი ან საპარლამენტო აპარატის წევრი, ხედავს თქვენს პაროლი, რომელსაც იყენებთ საიტზე შესასვლელად. არასწორი ხელში ასეთი ინფორმაცია არა მხოლოდ განაპირობებს თქვენი ანგარიშის შიგთავსის გამჟღავნებას, არამედ აძლევს შესაძლო თავდამსხმელებს, სადაც არ უნდა იყვნენ ისინი, კარგ წარმოდგენას იმის შესახებ, თუ რას აკეთებთ ან ფიქრობთ.

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):



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 პარლამენტი შეშფოთებულია თქვენს ონლაინ საქმიანობაზე მიზანმიმართული თვალთვალის გამო და განიცდის მკაცრ ონლაინ ცენზურას (როგორიცაა ვებგვერდების და აპების ბლოკირება), შესაძლოაკონფიდენციალური, გსურდეთ სანდო ვირტუალური ქსელის (VPN) 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.

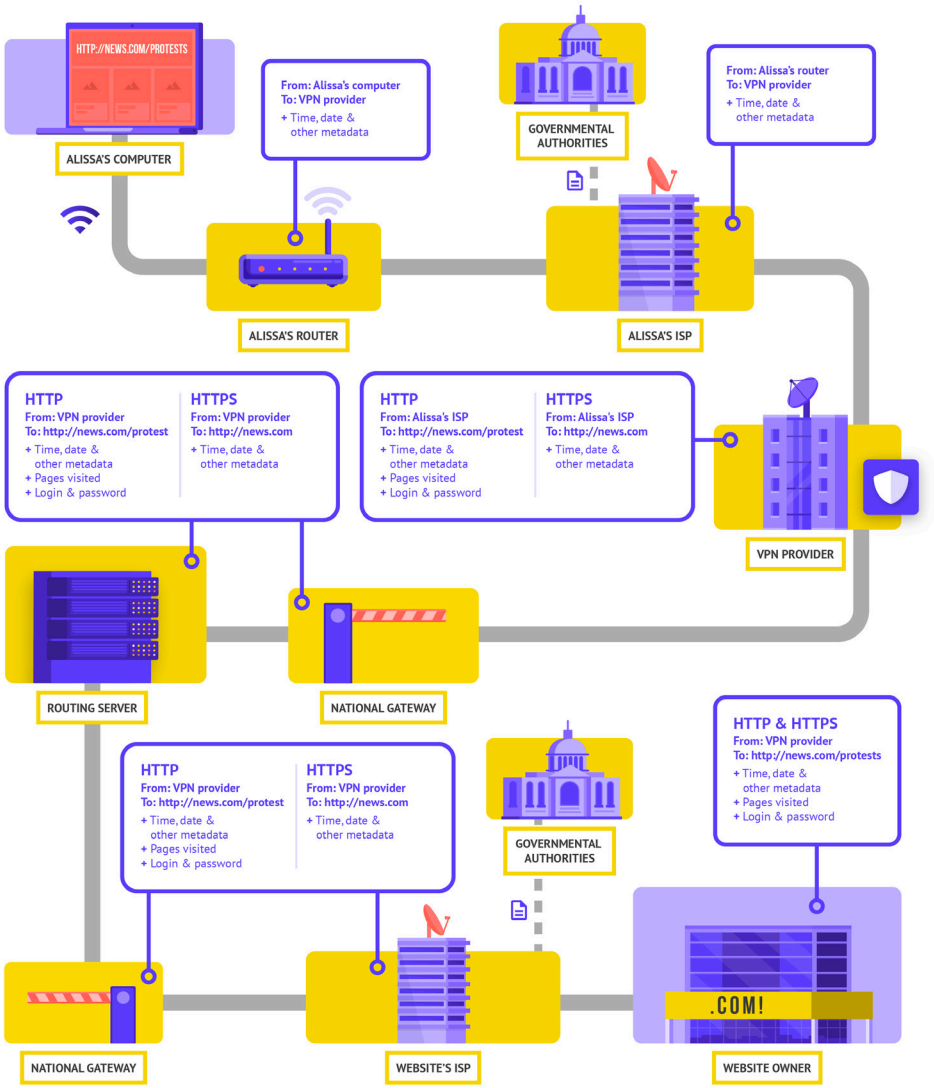
თუ **გაინტერესებთ**, DNS-ი ნიშნავს დომენის დასახელების სისტემას. რეალურად, ესაა ინტერნეტის ტელეფონის ნომრების წიგნაკი, რომელიც გარდაქმნის ადამიანისათვის მოსახერხებელ დომენის დასახელებებს (მაგალითად, ndi.org) ქსელისათვის მოსახერხებელ ინტერნეტ-პროტოკოლის (IP) მისამართებად. ეს საშუალებას აძლევს ადამიანებს 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 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 პარლამენტის თანამშრომლებს 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?

VPN 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. დიდ ორგანიზაციებში, როგორიცაა პარლამენტი, „ბიზნესი“ ან „კორპორატიული“ VPN ხშირად გამოიყენება შიდა სისტემებსა და აპლიკაციებზე წვდომის მთლიანობის დასაცავად (როგორიცაა დისტანციურად ხმის მიცემა). მიუხედავად იმისა, იყენებთ პერსონალურ VPN-ს თუ VPN-ს, რომელიც შექმნილია საქმიანი მიზნებისთვის, თქვენი ინტერნეტ ტრაფიკის დაცვის კონცეფცია ძირითადად ერთნაირად მუშაობს და მაინც მნიშვნელოვანია HTTPS-ის გამოყენება (თუნდაც VPN-ით სარგებლობდეთ). ასევე ძალიან მნიშვნელოვანია დარწმუნდეთ, რომ ენდობით VPN-ს, რომელსაც თქვენი პარლამენტი იყენებს. აი მაგალითი იმისა, თუ როგორ გამოიყურება VPN-ით ბრაუზინგი:



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.**

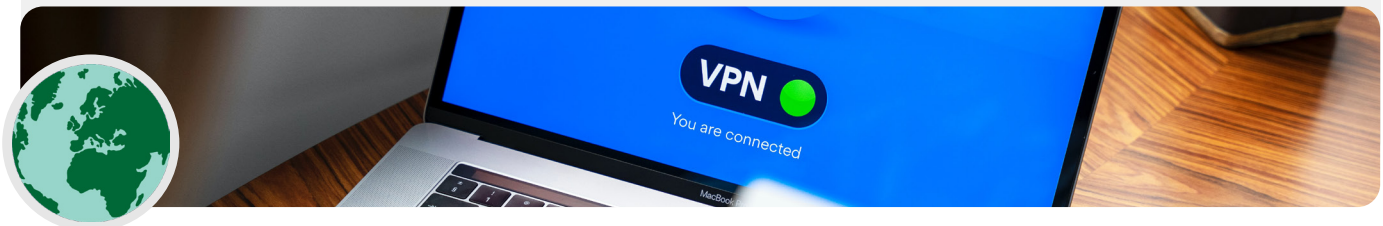
რატომ არ უნდა გამოიყენოთ უბრალოდ უფასო VPN-ი? მოკლე პასუხი ისაა, რომ უფასო VPN-ების უმეტესობა, მათ შორის, ისინი, რომლებიც წინასწარაა ინსტალირებული ზოგიერთ სმარტფონში, შეიცავს ხაფანგს. ყველა ბიზნეს- და სერვის-პროვაიდერის მსგავსად, VPN-ემა თავად უნდა შეინახოს თავი. თუ VPN-ი არ ყიდის საკუთარ სერვისს, როგორ 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, ირანელებმა აღმოაჩინეს პოპულარული VPN-ის „უფასო“ (მაგრამ ყალბი) ვერსია, რომელზე ინფორმაციაც ვრცელდებოდა ტექსტური შეტყობინებების საშუალებით. უფასი VPN (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 უნდა გამოვიყენოთ?

თუ საპარლამენტო ინტერნეტ ტრაფიკის უზრუნველყოფის გარდა, თქვენ ასევე გჭირდებათ გამოსავალი, რომ უსაფრთხოდ შეზღუდოთ წვდომა შიდა საპარლამენტო სისტემებსა და აპლიკაციებზე მხოლოდ თქვენს საპარლამენტო ქსელში (თუნდაც დისტანციურად მუშაობის დროს), შეგიძლიათ დანერგოთ „ბიზნეს“ ან „კორპორატიული” VPN. არსებობს მრავალი ტექნოლოგა, რომელიც შეგიძლიათ განიხილოთ, მათ შორის: **AnyConnect** Cisco-სგან, **Global Protect** PaloAlto-სგან ან **Access** Cloudflare-სგან (ტექნიკურად ნულოვანი ნდობის წვდომის სისტემა და არა VPN). ნებისმიერ შემთხვევაში, ასეთი სისტემები მოითხოვს გამოცდილ IT პერსონალს დანერგვისა და სისტემის ეფექტური მართვისთვის.

თუ მოწინავე „კორპორატიული“ VPN არის ძალიან ბიუჯეტური ან ძალიან რთული თქვენი პარლამენტისთვის, ყველა წევრისა და თანამშრომლისთვის შეგიძლიათ ასევე განიხილოთ პერსონალური VPN პარამეტრების გამოყენება, როგორიცაა **ProtonVPN** ან **TunnelBear** (რაც ასევე გთავაზობთ Teams-ის გეგმას ანგარიშის მართვის გასამარტივებლად) კიდევ ერთი ოფციაა თქვენი საკუთარისერვერის კონფიგურაცია Jigsaw-ის **Outline-ის** გამოყენებით, სადაც თქვენს პროფილს მართავს არა კომპანია, არამედ თქვენ თავად უნდა გამართოთ თქვენი საკუთარი სერვერი.

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

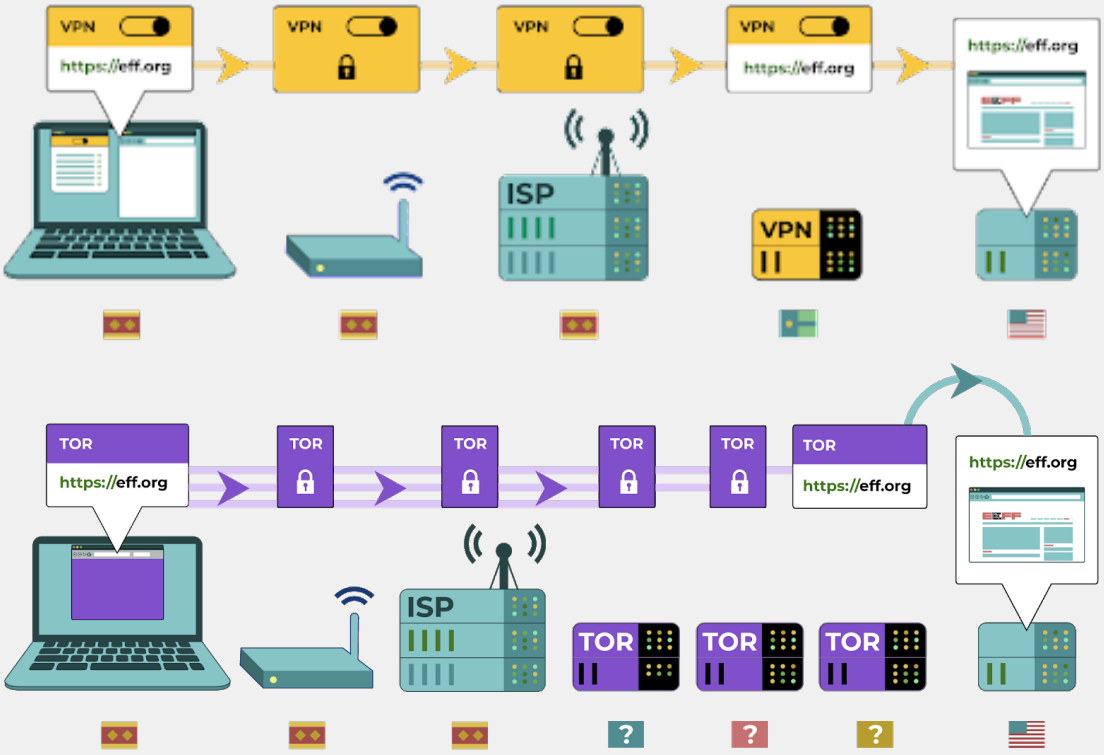
გარდა VPN-ებისა, შესაძლოა გაგიგონიათ Tor-ის, როგორც ინტერნეტის გამოყენებისას მეტი უსაფრთხოების ინსტრუმენტის შესახებ. მნიშვნელოვანია გვესმოდეს, რა არის ორივე და რატომ გსურთ გამოიყენოთ ერთი ან მეორე.

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, 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**, რათა ამუშაოს Tor 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 არაა მეტად ფართოდ გავრცელებული ინსტრუმენტი და, ამდენად, გამოირჩევა მეტოქეებისათვის, რომლებიც შესაძლოა აწარმოებდნენ თქვენი ინტერნეტ-ტრაფიკის მონიტორინგს.

ასე რომ, მიუხედავად იმისა, რომ ალბათ ძალიან ცოტა შემთხვევაა, როდესაც Tor-ს გამოყენება საჭიროა საპარლამენტო კონტექსტში, თუ თქვენ ან ვერ იყიდით სანდო VPN-ს, ან აღმოაჩენთ, რომ თქვენი პარლამენტი მუშაობს ისეთ გარემოში, სადაც VPN-ები რეგულარულად იბლოკება, Tor შეიძლება იყოს კარგი ვარიანტი. თუ ეს კანონიერია, შეზღუდოს თვალთვალის გავლენა და თავიდან აიცილოს ცენზურა ინტერნეტში.

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

გარდა რეპუტაციის არმქონე VPN-ის სერვისის გარშემო შეშფოთებისა, გასათვალისწინებლად უდიდესი მნიშვნელობა აქვს მიიპყრობს თუ არა VPN-ის ან Tor-ის გამოყენება არასასურველ ყურადღებას ან 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 ან VPN. 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 ან, განსაკუთრებით, Tor (რომელიც გაცილებით ნაკლებად გამოიყენება და, ამდენად, უფრო მეტად „საგანგაშოა“) არ წარმოადგენს სწორ არჩევანს თქვენი პარლამენტისთვის.

რომელ ბრაუზერს უნდა ვიყენებდეთ?

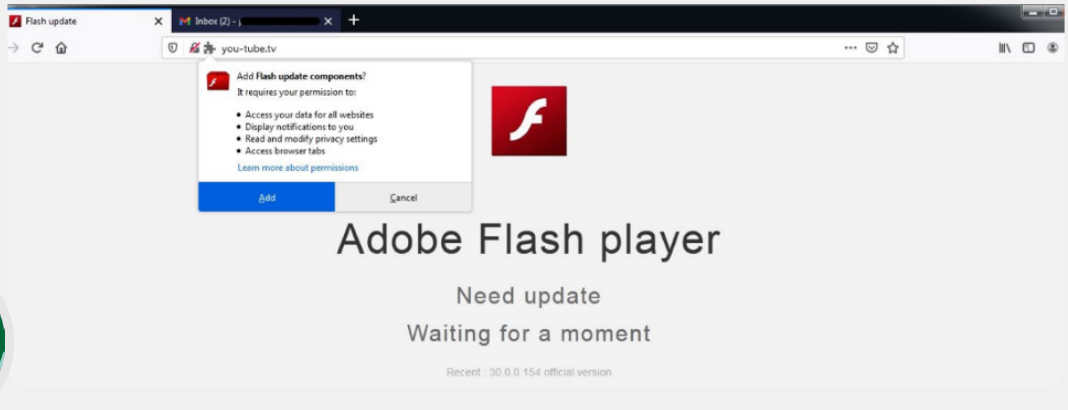
გამოიყენეთ ავტორიტეტული ბრაუზერი, როგორიცაა Chrome-ი, Firefox-ი, Brave-ი, Safari-ი, Edge-ი ან Tor Browser-ი. როგორც Chrome-ი, ისე Firefox-ი მეტად ფართოდ გამოიყენება და მშვენივრად მუშაობს უსაფრთხოების თვალსაზრისით. ზოგიერთი უპირატესობას Firefox-ს ანიჭებს კონფიდენციალურობაზე ორიენტირებულობის გამო. ნებისმიერ 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

აღნიშნული ბრაუზერის გაფართოებით ან დანამატით შეტევები შესაძლოა ისევე დამაზიანებელი იყოს, როგორც საზიანო პროგრამა, გაზიარებული უშუალოდ ფიშინგური ჩამოტვირთვების ან სხვა პროგრამული უზრუნველყოფის საშუალებით. მაგალითად, **ოსტატურად შექმნილ მავნე დახმარე პროგრამას** სახელწოდებით „Flash Update Components" სამიზნეში ჰყავდა აყვანილი ტიბეტის პოლიტიკურ ორგანიზაციები 2021 წლის დასაწყისში. დამხმარე პროგრამა აჰყვებოდა ხოლმე მომხმარებლებს, რომლებიც სტუმრობენ ფიშინგ ელფოსტასთან დაკავშირებულ ვებსაიტებს და დაინსტალირების შემდეგ ის ჰაკერებს საშუალებას აძლევდა მოეპარათ ელექტრონული ფოსტა და მონაცემები.

ბრაუზერის დამხარე პროგრამა ასევე შეიძლება იყოს საპარლამენტო რესურსების, როგორიცაა ვებსაიტების დაინფიცირების ვექტორი, რომელსაც, თავის მხრივ შეუძლია მავნე პროგრამის გავრცელება საიტის ვიზიტორების ფართო სპექტრზე (მათ შორის ფართო საზოგადოებაზე, პარლამენტის თანამშრომლებზე და თავად წევრებზე). მაგალითად, ავიღოთ ჰაკერების მიერ პოპულარული ბრაუზერის დამხმარე პროგრამა Browsealoud (ახლა ცნობილია როგორც ReachDeck), რომელიც გარდაქმნის ვებსაიტის ტექსტს აუდიო ჩანაწერად მხედველობის დაქვეითებული მომხმარებლებისთვის. 2018 წელს ჰაკერებმა შეიტანეს მავნე კოდი ბრაუზერის დამხმარე პროგრამაში, რომელიც გამოიყენებოდა სხვადასხვა სამთავრობო უწყების ვებსაიტებზე, მათ შორის **ვიქტორიას შტატის პარლამენტში ავსტრალიაში**. ბრაუზერის ინფიცირებული დამხმარე პროგრამის დახმარებით და არასწორი კონფიგურაციის შემდეგ, ვებსაიტის ვიზიტორების მოწყობილობები დაინფიცირდა მავნე პროგრამით, როდესაც ისინი საიტს სტუმრობდნენ. ამ შემთხვევაში, მავნე პროგრამა გამოიყენებოდა მოწყობილობების გამოსაყენებლად კრიპტოვალუტის მაინინგისთვის, მაგრამ ასეთი ტაქტიკა ჰაკერებს შეეძლოთ გამოეყენებინათ მავნე პროგრამების გასავრცელებლად მონაცემების მოპარვის ან ჯაშუშობის მიზნით.



სოციალური მედიის უსაფრთხოება

პარლამენტის თანამშრომლებს და წევრებს ბევრი აქვთ ხოლმე სათქმელი - და ზოგჯერ იმაზე მეტი, ვიდრე უდნათ - სოციალურ მედიაში გამოქვეყნებითა და კომენტარებით.

იქნება ეს Facebook-ი, Twitter-ი, Instagram-ი, YouTube-ი თუ რეგიონისათვის 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 ეხება არა მხოლოდ პარლამენტების ოფიციალურ გვერდებს, არამედ ზოგიერთ შემთხვევაში თანამშრომლების, ასევე მათი ოჯახებისა და მეგობრების პირად ანგარიშებს.

სოციალური მედიის უსაფრთხოება და პარლამენტები

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 ჰაკერებმა ყველაფერი გააკეთეს იმისათვის, რომ რამდენიმე ათასი დოლარი გამოიმუშავეს ცხოველთა თავშესაფრიდან, თქვენ წარმოიდგინეთ, რა ზიანი შეიძლება მიაყენონ დახვეწილმა მეტოქეებმა, თუ ისინი მოიპოვებენ წვდომას თქვენს საპარლამენტო ანგარიშებზე ან წარმატებულად გამოიყენებენ ცნობილი პარლამენტის წევრის ან თანამშრომელის ანგარიშს ონლაინ.

სოციალური მედიის ანგარიშების გატეხვის გარდა, საპარლამენტო ვებსაიტები ასევე ხშირი სამიზნეა მათი ცნობადობისა და რეპუტაციის გათვალისწინებით. მაგალითად, 2017 წელს, ავსტრიის პარლამენტის ვებგვერდი დაბლოკა ჰაკერების ჯგუფმა, რომლებიც, სავარაუდოდ, უკმაყოფილო იყვნენ იმ დროისთვის თურქეთთან ქვეყნის გაუარესებული ურთიერთობებით.

საპარლამენტო სოციალური მედიის პოლიტიკის შემუშავება

ჩავთვალოთ, რომ სოციალურ მედიაში გამოქვეყნებული ნებისმიერი რამ შეიძლება გახდეს საჯარო და შესაბამისად გამოყენებული იქნებს საპარლამენტო სოციალური მედიის პოლიტიკაში. ბევრი საპარლამენტო სამუშაოს საჯარო ბუნების გათვალისწინებით, სავარაუდოა, რომ გსურთ პოსტებისა და შეტყობინებების უმეტესობის საჯაროდ გამოქვეყნება, მაგრამ მაინც მნიშვნელოვანია დასვათ და უპასუხოთ კითხვებს, როგორიცაა: ვის აქვს წვდომა სოციალურ მედიაში თქვენს პროფილებზე? ვის აქვს უფლება გამოაქვეყნოს პოსტები და ვის ესაჭიროება პოსტების დადასტურება? რას იტყვით კომენტარებსა და პრაქტიკაზე? რა ინფორმაცია უნდა/არ უნდა გაზიარდეს სოციალურ მედიაში? თუ აქვეყნებთ ფოტოებს, მდებარეობის ინფორმაციას ან სხვა საიდენტიფიკაციო ინფორმაციას თქვენი თანამშრომლების, წევრების ან პარტნიორების შესახებ, სთხოვეთ მათ ნებართვა და გაითვალისწინეთ რაიმე შესაძლო რისკი? ასეთი კითხვები განსაკუთრებით მნიშვნელოვანია, თუ თქვენი პარლამენტი საჯაროდ აკავშირებს მოქალაქეებს სოციალური მედიის ან მსგავსი ონლაინ საჯარო ჩართულობის პორტალების მეშვეობით.
გარდა თქვენი პოლიტიკის შემუშავების და მისი პერსონალისთვის განმარტებისა, უზრუნველყავით თქვენი კონფიდენციალურობის და დაცვის (ხშირად „უსაფრთხოებად“ ხსენებული) პარამეტრების სწორი კონფიგურაცია. რამდენიმე ძირითადი კითხვა, რომელიც უნდა დაუსვათ საკუთარ თავს, როდესაც გადაწყვეტთ, რომელი კონფიდენციალურობისა და უსაფრთხოების პარამეტრებია საუკეთესო საპარლამენტო და პირადი ანგარიშებისთვის, 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 გიპოვონ ადამიანებმა ელფოსტის მისამართით ან (პირადი თუ საქმიანი) ტელეფონის ნომრით?
- 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**, **Twitter**, **Instagram** და **YouTube**. 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 პარლამენტის სოციალური მედიის ანგარიშები ისეთივე უსაფრთხოა, როგორც მასთან „დაკავშირებული“ ანგარიშები. ეს განსაკუთრებით მნიშვნელოვანია გვახსოვდეს Facebook-ის შემთხვევაში, სადაც სხვის დაკავშირებულ პირად ანგარიშს შეუძლია თქვენი გვერდების მართვა.

ონლაინ დევნა

სამწუხაროდ, ბევრი პარლამენტი და მათთან დაკავშირებული ჯგუფები განიცდიან მნიშვნელოვან ონლაინ შევიწროებას, 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. NDI-ს Gender, Women, and Democracy-ის ჯგუფის ანგარიშის თანახმად **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.

რამდენადაც თქვენი პარლამენტი ავითარებს თავის სოციალურ მედია პოლიტიკას, მნიშვნელოვანია, რომ თვალყური ადევნოთ ამ 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 პარლამენტის ფარგლებში, მათ შორის, აწარმოეთ საკუთარი პერსონალის კვლევა, რათა გაიგოთ როგორ მოქმედებს ონლაინ დევნა მათზე და შექმნათ სწრაფი რეაგირების ჯგუფი, რათა დაეხმაროთ თანამშრომლებს 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 ან/და **პრობლემურ ანგარიშებზე ინფორმირების (რეპორტინგის)** პრაქტიკა უშუალოდ პლატფორმებთან.

იმ წევრებთან ან პერსონალთან ურთიერთობისას, რომელიც ონლაინ (თუ რეალურ სამყაროში) გამხდარა 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 დაუკავშიროთ 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 შესაძლებლობის დაცვისა, ასევე მნიშვნელოვანია ყველაფერი გააკეთოთ, რათა უზრუნველყოთ თქვენი პარლამენტის 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 მიმართავს თქვენს სერვერს საზიანო ტრაფიკის შექმნის მიზნით. DDoS დაცვის რამდენიმე ვარიანტი - რაც ართულებს მოწინააღმდეგისთვის თქვენი ვებსაიტის წაშლას - მოიცავს **Cloudflare**, Amazon-ის **AWS Shield** ან eQualitie-ის **Deflect** სერვისს.

თქვენი პარლამენტისთვის უსაფრთხო ვებ ჰოსტინგი

ვებგვერდები განთავსებულია კომპიუტერებში - ისინი კი მოწყვლადია ჰაკერების მიმართ ზუსტად ისე, როგორც თქვენი საკუთარი მოწყობილობები. თუ შესაძლებელია, თქვენმა პარლამენტმა უნდა ისარგებლოს არსებული ჰოსტინგის სერვისებით, როგორიცაა WordPress, Wix ან სხვა, რომლებიც თქვენს მაგივრად მართავენ საიტის მთელ უსაფრთხოებას. თუ თქვენი ვებგვერდის საჭიროებები უფრო კომპლექსურია ან თუ გესაჭიროებათ თქვენი ვებგვერდის თავად ჰოსტინგი, კონცენტრაცია მოახდინეთ თქვენი ოპერაციული სისტემის და ვებ-ჰოსტინგის პროგრამული უზრუნველყოფის მუდმივ განახლებას 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 ზედპირს და შეტევებისადმი უფრო მედეგს 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 სტუმრებისთვის განკუთვნილი ქსელის შექმნა პარლამენტის შენობებში, თუ სტუმრები შემოდიან შენობაში და გადიან და იყენებენ ინტერნეტს.

უსაფრთხოების დაცვა ინტერნეტში

- **ჩაატარეთ რეგულარული ტრენინგი წევრებისა და თანამშრომლებისთვის ვებ უსაფრთხოების ძირითადი პრაქტიკის დაცვის მნიშვნელობის შესახებ.**
- **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 თქვენთვის მისაღებია, აირჩიეთ სანდო, ასწავლეთ თქვენს პერსონალს მისი გამოყენება და დარწმუნდით, რომ მას ყოველთვის იყენებენ.**
- **შეიმუშავეთ და გაუკეთეთ დისტრიბუცია სოციალური მედიის გამოყენების შესახებ მკაფიო საპარლამენტო პოლიტიკას.**
- **ჩართეთ კონფიდენციალურობის და უსაფრთხოების პარამეტრები სოციალური მედიის ყველა პროფილში.**
- **გაანალიზეთ ონლაინ შევიწროების შედეგები და მოემზადეთ დაზარალებული წევრებისა და თანამშრომლების დასახმარებლად.**
- **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 სტუმრების ქსელი თქვენს ადგილობრივ Wi-Fi ქსელზე წვდომისთვის.**

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. ეს მოიცავს ქაღალდის დოკუმენტებს; საპარლამენტო ოფისებს; კამერებს ან სამუშაო ადგილებს; და, რა თქმა უნდა, თქვენ, თქვენს თანამშრომლებს და წევრებს.

ფიზიკური უსაფრთხოება და პარლამენტი

სამწუხაროდ, პარლამენტებსა და სხვა საკანონმდებლო ორგანოებზე ფიზიკური თავდასხმები იშვიათი არაა და ხშირად მნიშვნელოვან გავლენას ახდენს როგორც ფიზიკურ, ისე ინფორმაციულ უსაფრთხოებაზე. 2021 წლის 6 იანვარს, ამბოხებულები შეიჭრნენ შეერთებული შტატების კაპიტოლიუმის შენობაში - სადაც განთავსებულია აშშ-ს საკანონმდებლო ორგანოს ორივე პალატა - საპრეზიდენტო არჩევნების შედეგების გამოქვეყნების შეჩერების მიზნით. ფიზიკური თავდასხმის შედეგად ტრაგიკულად დაიღუპა ხუთი პირი და მნიშვნელოვანი ფსიქოლოგიური სტრესი მიიღეს კონგრესის წევრებმა და თანამშრომლებმა. თუმცა ეს არ იყო ერთადერთი უარყოფითი ფაქტი. თავდამსხმელებმა ასევე გაანადგურეს IT აღჭურვილობა, მოიპოვეს წვდომა წევრების ოფისებში სენსიტიურ მასალებზე და, ალბათ, რაც ყველაზე საზიანოა, მოიპარეს კომპიუტერები და სხვა მოწყობილობები პოტენციურად კონფიდენციალური ინფორმაციით აშშ-ს კაპიტოლიუმიდან.

მგრძნობიარე ნაწილების საინფორმაციო საშუალებები (SCIF)

უაღრესად მგრძნობიარე საუბრების გასამართად, ზოგიერთმა პარლამენტმა უზრუნველყო ფიზიკური ოთახები, სახელწოდებით SCIF. ეს სივრცეები შექმნილია ისე, რომ სენსიტიური ინფორმაცია, როგორიცაა ეროვნულ უსაფრთხოებასთან ან დაზვერვასთან დაკავშირებული საკითხები, ნახოს და განიხილოს დეპუტატებსა და მათ თანამშრომლებს შორის გარე მეთვალყურეობის ან ჯაშუშობის გარეშე. გარდა სათანადო ფიზიკური კონსტრუქციისა, სათანადო SCIF მოითხოვს, რომ ადამიანებმა დატოვონ მოწყობილობები (როგორიცაა მობილური ტელეფონები) ოთახის გარეთ, სანამ დისკუსიაზე შევიდნენ.

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. იმისთვის, რომ ქურდობა გაძნელდეს, აუცილებლად დააინსტალირეთ ძლიერი საკეტები (და შეცვალეთ ისინი პერსონალის სამსახურიდან წასვლის დროს) პარლამენტის და/ან სახლის შენობებზე. გარდა ამისა, იფიქრეთ ლეპტოპის სეიფის ან ჩასაკეტი კარადის ყიდვაზე მოწყობილობების ღამით დასაცავად. აღნიშნულმა უსაფრთხოების 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 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!

ამ ტექნიკურ ნაბიჯებამდე დაუთმეთ დრო პარლამენტში არსებული ყველა ტექნიკის ინვენტარიზაციას. თუ არ გაქვთ ყველა თქვენი მოწყობილობის სია, უფრო რთულია იმის აღრიცხვა, თუ რა დაგაკლდათ ერთ-ერთის ქურდობის შემთხვევაში.

რა ვუყოთ ამდენ ქაღალდს?

არსებობს დიდი ალბათობა, რომ თქვენს პარლამენტს გააჩნდეს დიდი ოდენობით ინფორმაცია, რომელიც დაბეჭდილია ქაღალდზე, ჩაწერილია ბლოკნოტებში ან ჩანიშნულია სტიკერებზე. ზოგიერთი მათგანი შეიძლება იყოს ძალიან სენსიტიური, როგორიცაა კონფიდენციალური ჩვენების ჩანაწერები ან პირადი შეხვედრები. 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. შეინახეთ კრიტიკული ინფორმაცია ნაკლებად თვალშისაცემ, კარგად დაცულ ადგილას.

რამდენადაც შესაძლებელია, ეცადეთ მოიცილოთ არასაჭირო ინფორმაციის ამონაბეჭდები. გახსოვდეთ: შეუძლებელია იმის მოპარვა, რაც არ გაქვთ. დანიშნეთ პარლამენტის გამომძიებელი ნაბეჭდი ჩანაწერების შენახვის საკითხში და დარწმუნდით, რომ შეაგროვეთ ნებისმიერი ქაღალდის ჩანაწერი თანამშრომლებისგან, თუ ისინი გადაწყვეტენ ან გაათავისუფლებენ ორგანიზაციიდან, ისევე როგორც თქვენ შეაგროვებთ პარლამენტის მიერ გამოცემულ 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.

საპარლამენტო პოლიტიკა

მიუხედავად იმისა, რომ ბევრისთვის „ოფისის“ რეალობა მნიშვნელოვნად შეიცვალა COVID-19 პანდემიის დაწყების შემდეგ, პარლამენტისთვის მაინც მნიშვნელოვანია მკაფიო პოლიტიკის დადგენა შენობებში წვდომასთან დაკავშირებით. 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.

მარტივ, მაგრამ მნიშვნელოვან კითხვაზე პასუხის გასაცემა აუცილებელია, თუ ვის აქვს ოფისის გასაღები ან წვდომა სამკერდე ნიშანზე. გასაღები უნდა ჰქონდეს მხოლოდ სანდო პერსონალს, ხოლო საკეტები უნდა იცვლებოდეს, როცა პერსონალი მიდის ან/და გარკვეული პერიოდულობით. დღის განმავლობაში, ნებისმიერი კარი, რომელიც არ არის ჩაკეტილი, მუდმივი უნდა იყოს სანდო და/ან დაცვის თანამშრომლის თვალწინ. გარდა ამისა, დარწმუნდით, რომ თქვენს პარლამენტს აქვს სანდო ურთიერთობა სერვისის პროვაიდერებთან, როგორიცაა დასუფთავების პერსონალი და გარე ტექნიკოსები, რომლებსაც აქვთ წვდომა შენობაში. 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.

ნებადართულია თუ არა ამომრჩეველი თქვენს პარლამენტში? შესაძლოა, საზოგადოებას აქვს პარლამენტის შენობის ნაწილებზე წვდომის უფლება? 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

პარლამენტის ფიზიკური უსაფრთხოების მოსალოდნელმა რისკებმა შეიძლება გავლენა იქონიოს თანამშრომლებზეც. 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 წევრების და თანამშრომლების ცხოვრებაზე. NDI-ის **#Think10** Safety Planning Tool არის სასარგებლო რესურსი პოლიტიკურად აქტიური ქალებისთვის, რომლებიც შესაძლოა იმყოფებოდნენ გაზრდილი რისკის ქვეშ პარლამენტში და ზოგადად პოლიტიკაში მონაწილეობის 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-ს **ონლაინ სავალე შევიწროების სახელმძღვანელო** შეიცავს იდეებს იმის შესახებ, თუ როგორ შეუძლიათ ორგანიზაციებს დაეხმარონ პერსონალს კრიზისის დროს და მის შემდეგ.

უსაფრთხოება მოგზაურობის დროს

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.

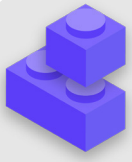
გარდა მოგზაურობისათვის მომზადების და მოგზაურობისას თქვენს მიერ გაზიარებული მონაცემების მინიმიზაციისა, არსებობს რამდენიმე უმნიშვნელოვანესი ოპერაციული რჩევა, რომლებიც უნდა გაიაზროთ და ჩართოთ თქვენს მოგზაურობის ორგანიზაციულ პოლიტიკაში.

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.
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 პარლამენტისთვის

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.



თქვენი ფიზიკური უსაფრთხოების დაცვა

- **შეახსენეთ წევრებს და თანამშრომლებს, რომ მოწყობილობები ყოველთვის ფიზიკურად დაცული იყოს.**
- **შეამოწმეთ და დაიცავით ყველა გზა, რომლითაც ადამიანებს შეუძლიათ თქვენს შენობაში შეღწევა.**
- **შეიმუშავეთ სტუმრისა და წვდომის პოლიტიკა.**
- **გამოიყენეთ მტკიცე საკეტები, პირადობის მოწმობის/ბეჯების სისტემები და საჭიროების შემთხვევაში შეცვალეთ/განაახლეთ ისინი.**
- **განიხილეთ კამერების ან სხვა შიდა უსაფრთხოების სისტემების დაყენება**
- **იქონიეთ და გამოიყენეთ ქაღალდის გამანადგურებელი.**
  - 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 საპარლამენტო მოგზაურობის პოლიტიკა.**
- **დარწმუნდით, რომ თანამშრომლებმა იციან რა უნდა გააკეთონ მოგზაურობის დროს საგანგებო სიტუაციის შემთხვევაში.**
- **არ დაგავიწყდეთ დამატებითი მონაცემები, რომლებიც იქმნება და გაზიარდება მოგზაურობის თუ ღონისძიებების ორგანიზებისას.**

რა უნდა გააკეთდეს, როდესაც რაღაც ცუდი ხდება

ამგვარად, იცით როგორ უნდა მოიქცეთ სწორად. თქვენ დანერგეთ პოლიტიკები და ჩაუტარეთ ტრენინგი ყველას პარლამენტში საუკეთესო პრაქტიკის შესახებ. მიუხედავად ხსენებული რთული საქმისა, მეტად სავარაუდოა, რომ საბოლოოდ რაღაც არასწორად მოხდება.

ხდება. ამ დროს, უმნიშვნელოვანესია დანერგილი იყოს შემთხვევაზე რეაგირების გეგმა. შემთხვევაზე რეაგირება არის თქვენი პარლამენტის უსაფრთხოების გეგმის მნიშვნელოვანი და ხშირად დაუფასებელი ნაწილი, რადგან ეს შეიძლება იყოს განსხვავება თავდასხმას შორის, რომელიც ანადგურებს თქვენს რეპუტაციას ან უსიამოვნო დარტყმა მიმავალ გზაზე. გახსოვდეთ, რომ შემთხვევაზე რეაგირება შეგიძლიათ მხოლოდ მაშინ, როცა იცით მის შესახებ. ძალიან მნიშვნელოვანია უსაფრთხოების ძლიერი კულტურის არსებობა და წევრებისა და პერსონალის წახალისება, რომ შეატყობინონ პრობლემების შესახებ. ამიტომაა უკეთესი დაჯილდოვდეს უსაფრთხოების თვალსაზრისით სწორი ქცევა, ვიდრე დაისაჯოს 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 ჩვენი ელ-შეტყობინებები ან სენსიტიური დოკუმენტების უმეტესობა მოიპარეს და გამჟღავნდა?
- როგორ ვიქცევით, თუ ჩვენი ელ-შეტყობინებები ან სენსიტიური დოკუმენტების უმეტესობა მოიპარეს და გამჟღავნდა?
- რა ვქნათ, თუ ჩვენს ერთ-ერთ თანამშრომელს ფიზიკური საფრთხე დაემუქრება? ან თუ ისინი ებრძვიან სტრესს და მოუსვენრობას ხსენებული საფრთხეების გამო?
- როგორ ვიქცევით, თუ ოფისი დაზიანდა ხანძრის, წყალდიდობის ან სტიქიური უბედურების დროს?
- რა ვქნათ, თუ წევრის კომპიუტერი ან ტელეფონი დაიკარგა ან მოიპარეს?

ამ და სხვა კითხვებზე პასუხები პარლამენტის მიერ განსხვავებული იქნება, მაგრამ მნიშვნელოვანია მათზე ერთად ვიფიქროთ და მკაფიოდ ჩამოვაყალიბოთ და გავუზიაროთ გეგმა, რათა ყველა მზად იყოს დაუყოვნებლივ მიიღოს ზომები ზიანის შესამცირებლად.
Tactical Tech-ის [„ყოვლისმომცველი უსაფრთხოების სახელმძღვანელოს“]() თანახმად, ინციდენტზე რეაგირების გეგმის დასაწყებად კარგი პოზიციაა თქვენი ორგანიზაციის კონტექტსში **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 სიტუაციებში ამ მნიშვნელოვანია სტრატეგიის ფარგლებში დამხმარე ქსელის გააქტიურება - მოკავშირეთა ფართო ქსელი, რომელიც შეიძლება მოიცავდეს თქვენი ხელისუფლების სხვადასხვა შტოებს, სხვა მეგობრულ მთავრობებს, ტექნოლოგიურ კომპანიებს, უსაფრთხოების სერვისის მომწოდებლებს და მრავალმხრივ ინსტიტუტებს, რომ დავასახელოთ მხოლოდ რამდენიმე მაგალითი. 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 შემთხვევის პარლამენტის რეპუტაციაზე გავლენა და მოემზადეთ შესაბამისი რეაგირებისთვის. დარწმუნდით, რომ პარლამენტის კომუნიკაციების ხელმძღვანელმა იცის შემთხვევის შესახებ და შეუძლია თვალყური ადევნოს სოციალურ მედიას ან სხვა მედიას პოტენციური გავლენის შესამცირებლად. 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.

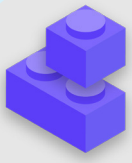
ადრეული განგაშის და რეაგირების სისტემის შექმნა

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 გქონდეს 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. როგორც პარლამენტი, თქვენ გაქვთ განსაკუთრებული ძალაუფლება და გამორჩეული პოზიცია, როდესაც საქმე ეხება ადგილობრივი მონაცემთა უსაფრთხოებისა და კონფიდენციალურობის რეგულაციების გაგებასა და პატივისცემას.
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 სიტუაციებზე რეაგირების გეგმის შედგენისას, ჩვენ მტკიცედ მოგიწოდებთ გამოიყენოთ რამდენიმე შესანიშნავი არსებული რესურსი, რომელიც შექმნილია იმისთვის, რომ დაეხმაროს ორგანიზაციებს საგანგებო სიტუაციებზე რეაგირებაში ნავიგაციაში. მიუხედავად იმისა, რომ ყველა ეს რესურსი არ არის შექმნილი სპეციალურად პარლამენტებისთვის, მათი შინაარსი მაინც ძალიან აქტუალურია. 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 საპარლამენტო საგანგებო სიტუაციაზე რეაგირების გეგმა და დანერგეთ პრაქტიკაში.**
  - კოლექტიურად იფიქრეთ შესაძლო საგანგებო სიტუაციებზე და მოემზადეთ რეაგირებისათვის მათ დადგომამდე.
- **დარწმუნდით, რომ პარლამენტში ყველამ იცის, როგორ დაუკავშირდებით და რა ტექნიკური ნაბიჯები იქნება გადადგმული საგანგებო სიტუაციის შემთხვევაში.**
- **დაუთმეთ დრო სამართლებრივი დაცვის თქვენი საშუალებების და ვალდებულებების შესწავლას.**
- **იყავით მზად, უზრუნველყოთ წევრებისა და პერსონალის ემოციური და სოციალური მხარდაჭერა, რომელიც მათ სჭირდებათ საგანგებო სიტუაციის შემდეგ.**

დანართი A: რეკომენდებული რესურსები

- Tactical Tech-ის ჰოლისტიკური უსაფრთხოების სახელმძღვანელო; Creative Commons Attribution-ShareAlike 4.0 საერთაშორისო ლიცენზიით.
  - თავი 2.4 - ჩვენი ინფორმაციის გაგება და კატალოგი
  - თავი 1.5 - გუნდებსა და ორგანიზაციებში საფრთხეების შესახებ კომუნიკაცია
  - თავი 3.4 - უსაფრთხოება ჯგუფებსა და ორგანიზაციებში
- The Electronic Frontier Foundation-ის უსაფრთხოების განათლების კომპანიონი ; Creative Commons Attribution 3.0 აშშ ლიცენზია
  - საფრთხის მოდელირების აქტივობის სახელმძღვანელოt
- Freedom of the Press Foundation-ის ფიშინგის პრევენციისა და ელექტრონული ფოსტის ჰიგიენის სახელმძღვანელო ; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზიით
- Freedom of the Press Foundation-ის ჩაკეტვის სიგნალის სახელმძღვანელო ; Creative Commons Attribution 4.0 საერთაშორისო ლიცენზიით
- Electronic Frontier Foundation-ის სათვალთვალო თავდაცვის (SSD) გზამკვლევი ; Creative Commons Attribution 3.0 აშშ ლიცენზია
  - რა უნდა ვიცოდე დაშიფვრის შესახებ?
  - კომუნიკაცია სხვებთან
  - VPN-ის არჩევა, რომელიც თქვენთვის შესაფერისია
- Front Line Defenders-ის გზამკვლევი ჯგუფური ჩატისა და კონფერენციის ინსტრუმენტების უსაფრთხოდ
- Tactical Tech-ის მონაცემთა დეტოქსის ნაკრები
  - შეუშვით უფლება: გააძლიერეთ თქვენი პაროლები
  - გაიუმჯობესეთ 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 და Frontline Defender-ის „უსაფრთხოება ყუთში“ ; Creative Commons Attribution-Share Alike 3.0 არაადაპტირებული ლიცენზია
  - დაიცავით თქვენი მოწყობილობა საზიანო პროგრამის და ფიშინგური შეტევებისაგან
  - დაიცავით ფიზიკური საფრთხეებისგან
- SANS-ის OMG! ბიულეტენი: შეაჩერეთ ეს საზიანო პროგრამა
- Apple-ის „წვდომა მოწყობილობაზე და მონაცემებზე, როცა პირადი უსაფრთხოება საფრთხეშია“
- გლობალური კიბერ ალიანსის კიბერუსაფრთხოების ინსტრუმენტების ნაკრები მისიაზე დაფუძნებული ორგანიზაციებისთვის
- Ford Foundation-ის კიბერუსაფრთხოების შეფასების ინსტრუმენტი

დანართი B: უსაფრთხოების გეგმის საწყისი კომპლექტი

გამოიყენეთ შემდეგი საწყისი ნაკრები, რომ გააკეთოთ შენიშვნები, როდესაც თქვენ და თქვენი პარლამენტი კითხულობთ სახელმძღვანელოს და აანალიზებთ მასალებს და განიხილეთ თანდართულ კითხვებს თქვენს კოლეგებთან, რათა დაეხმაროთ პროდუქტიული დისკუსიის წარმართვაში.

დარწმუნდით, რომ მიუთითეთ ძირითადი „შემადგენელი ბლოკები“ სახელმძღვანელოს თითოეულ ნაწილში, რათა უზრუნველყოთ მნიშვნელოვან თემების გაშუქება უსაფრთხოების გეგმის შედგენის დროს. სახელმძღვანელოს ბოლოს, შემადგენელი ბლოკები, პასუხები ამ სადისკუსიო კითხვებზე და თქვენი შენიშვნები უნდა იყოს წარმატებული უსაფრთხოების გეგმის საფუძველი.

უსაფრთხოების კულტურის დანერგვა

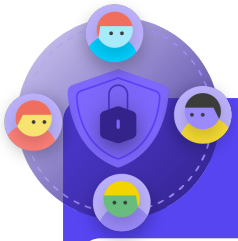
მყარი საფუძველი: ანგარიშებისა და მოწყობილობების დაცვა

მონაცემთა უსაფრთხო გადაცემა

უსაფრთხოების დაცვა ინტერნეტში

ფიზიკური უსაფრთხოების დაცვა

რა უნდა გააკეთდეს, როდესაც რაღაც ცუდი ხდება



უსაფრთხოების კულტურის დანერგვა

გასათვალისწინებელი კითხვები:

- როდის შეგიძლიათ დაგეგმოთ თქვენი უსაფრთხოების გეგმის განხილვა მთელ პარლამენტთან?
- რა დღეები ან დროა კარგი იმისთვის, რომ პარლამენტმა დაგეგმოს რეგულარული საუბრები და სწავლება უსაფრთხოების თემებზე?
- რა ნაბიჯების გადადგმა შეუძლია ხელმძღვანელობას უსაფრთხოების კარგი ქცევისა და უსაფრთხოების გეგმის მოდელირებისთვის? როგორ შეუძლიათ სხვებს პარლამენტში გარვეული როლი შეასრულონ უსაფრთხოების უზრუნველყოფაში?

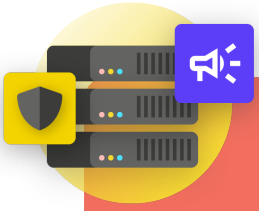
თქვენი შენიშვნები და იდეები:

მყარი საფუძველი: ანგარიშებისა და მოწყობილობების დაცვა

გასათვალისწინებელი კითხვები:

- როგორ გაატარებთ ანგარიშის უსაფრთხოების ზომებს - როგორიცაა პაროლის მენეჯერი და 2FA - პარლამენტში? რა წინააღმდეგობები შეიძლება შეგხვდეთ განხორციელები დროს?
- როგორ უზრუნველყოფს თქვენი პარლამენტი, რომ მოწყობილობები იყოს დაცული და განახლებულ მდგომარეობაში? ამის ფარგლებში, დასჭირდება თუ არა პარლამენტს არალიცენზირებული პროგრამული უზრუნველყოფის ან კომპიუტერების მოწესრიგების გეგმა?
- როდის არის კარგი დრო, რომ ყველა თანამშრომლისთვის მოაწყოთ ტრენინგი ფიშინგის, მავნე პროგრამების და მოწყობილობის უსაფრთხოების საუკეთესო პრაქტიკის საფრთხეების შესახებ?

თქვენი შენიშვნები და იდეები:

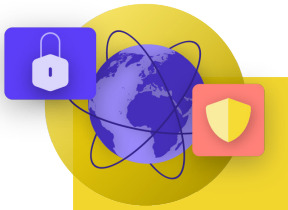


Communicating and Storing Data Securely

გასათვალისწინებელი კითხვები:

- როგორ გამოიყენებს პარლამენტი თავიდან ბოლომდე დაშიფრულ შეტყობინებებს უსაფრთხო კომუნიკაციის უზრუნველსაყოფად? რა წინააღმდეგობები შეიძლება შეგხვდეთ განხორციელები დროს?
- როგორ გამოიყენებს პარლამენტი ფაილების გაზიარების უსაფრთხო გადაწყვეტილებას როგორც შიგნით ასევე გარეთ? რა წინააღმდეგობები შეიძლება შეგხვდეთ განხორციელები დროს?
- როგორ გამოიყენებს პარლამენტი მონაცემთა უსაფრთხო შენახვისა და სარეზერვო კოპირების გადაწყვეტილებას? რა წინააღმდეგობები შეიძლება შეგხვდეთ განხორციელები დროს?

თქვენი შენიშვნები და იდეები:



უსაფრთხოების დაცვა ინტერნეტში

გასათვალისწინებელი კითხვები:

- როგორ გამოიყენებს პარლამენტი თანამშრომლებისთვის უსაფრთხო დათვალიერების მოთხოვნებს, როგორიცაა HTTPS, სანდო ბრაუზერი და, საჭიროების შემთხვევაში, VPN?
- რა იქნება პარლამენტის სოციალური მედიის პოლიტიკის ძირითადი ელემენტები? როგორ მოხდება მათი განხორციელება?
- როგორ დაიცავს პარლამენტი თავის ვებსაიტებსა და ვებ საკუთრებებს?

თქვენი შენიშვნები და იდეები:

ფიზიკური უსაფრთხოების დაცვა

გასათვალისწინებელი კითხვები:

- როგორ გაანაწილებს და განახორციელებს პარლამენტი სტუმრებისა და წვდომის პოლიტიკას?
- ვინ არის პასუხისმგებელი პერსონალის მომზადებაზე ფიზიკური და ციფრული უსაფრთხოების გამოწვევებისთვის, რომლებსაც ისინი შეიძლება შეხვდნენ სამსახურში მოგზაურობის დროს?
- რა ნაბიჯების გადადგმა შეუძლიათ თანამშრომლებს, რათა უზრუნველყონ თავიანთი მოწყობილობების უსაფრთხოება და უსაფრთხოება როგორც ოფისში, ასევე მოგზაურობის დროს?

თქვენი შენიშვნები და იდეები:

რა უნდა გააკეთოს, როცა რამე არასწორი ხდება

გასათვალისწინებელი კითხვები:

- როგორ გაანაწილებს და განახორციელებს პარლამენტი საგანგებო სიტუაციაზე რეაგირების პოლიტიკას?
- არის თუ არა ხელმისაწვდომი რესურსები პერსონალისთვის, რომელსაც შესაძლოა დასჭირდეს ემოციური და სოციალური მხარდაჭერა ინციდენტის შემდგომ? თუ არა, როგორ შეიძლება პარლამენტმა უზრუნველყოს ეს რესურსი ინციდენტის შემთხვევაში?

თქვენი შენიშვნები და იდეები:

დანართი C: გამოსახულების ციტატები

გვერდი 14: New York Times, “Australian Parliament Reports Cyberattack on Its Computer Network”, 2019, digital image, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html.
გვერდი 18: CNP Collection, “Security Protection Anti-Virus Software cms”, 2014, digital image, Alamy Stock Photo, 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 Bleeping Computers, “Norway parliament data stolen in Microsoft Exchange attack”, 2021, digital image, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
გვერდი 25: Cottonbro, “Person Holding Black and Silver Key”, 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
გვერდი 27: Blogtrepreneur, “Malware Infection”, 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
გვერდი 30: “Microsoft Loading Screen,” digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.
გვერდი 30: Mateuz Dach, “Turned-on iPhone and Displaying Icons,” 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
გვერდი 33: ZDNet, “Chinese hacking group impersonates Afghan president to infiltrate government agencies,” 2021, digital image, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
გვერდი 38: Andrew Keymaster, “People Gathering on Street During Daytime Photo,” 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
გვერდი 39: Surveillance Self-Defense, “No Encryption in Transit,” digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
გვერდი 40: Surveillance Self-Defense, “4.Transport-layer-alternate,” digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, “6. End-to-end Alternate”, digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
გვერდი 42: Surveillance Self-Defense, “9._endtoendencryptionmetadata,” 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
გვერდი 49: African News Agency, “Parliament meeting falls victim to hacking as MPs greeted by pornographic images,” 2020, digital image, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120
გვერდი 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
გვერდი 52: Brett Sayles, “Server Racks on Data Center,” 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
გვერდი 58: PhotoMIX Company, 2016, “White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky,” digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
გვერდი 63: Stefan Coders, “laptop-screen-vpn-cyber-security,” 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
გვერდი 65: Surveillance Self-Defense, “Using the Tor Browser,” digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
გვერდი 67: Nathan Dumlao, “White Samsung Android Smartphone on Brown Wooden Table,” 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
გვერდი 72: Matt Artz, “Two Broken 6-Pane On White Painted Wall Photo,” digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE