ციფრული მხარდაჭერა და უსაფრთხოება

ციფრული მხარდაჭერა და უსაფრთხოება ერთ-ერთი მნიშვნელოვანია იმ მრავალ გამოწვევას შორის, რომლის წინაშეც მედიაორგანიზაციები აღმოჩნდნენ კორონავირუსის პანდემიის პირობებში.

გაზრდილმა მოთხოვნამ ინფორმაციაზე, გაზარდა დატვირთვა მედიასაშუალებების ვებგვერდებზე და მენეჯერებს უწევთ იზრუნონ ტექნიკურ უზრუნველყოფაზე. მეორე მხრივ კი, დისტანციური ჟურნალისტიკის გამო, როდესაც სამუშაო პროცესი მთლიანად ონლაინ სივრცეშია გადასული, მედიაორგანიზაციებისთვის განსაკუთრებით მნიშვნელოვანია ორგანიზაციისა და თითოეული თანამშრომლის სხვადასხვა ონლაინ არხის, პლატფორმების, მეილების, სოციალური ქსელების ანგარიშების, მოწყობილობების, ასევე, ინფორმაციის წყაროების ჰაკერებისგან, ე.წ ფიშინგისა და სხვა კიბერსაფრთხეებისგან დაცვა.

ციფრული მხარდაჭერა

პანდემიის პირობებში, იზრდება მოთხოვნა ინფორმაციაზე - ამას ხელს ისიც უწყობს, რომ საგანგებო მდგომარეობისას ადამიანების შესაძლო აქტივობა მაქსიმალურადაა შეზღუდული და გარე სამყაროსთან კავშირი უმეტესწილად სწორედ საინფორმაციო საშუალებებით ხდება. ამიტომ, პანდემიის პირობებში, მზად უნდა იყოთ თქვენს ვებ გვერდზე ვიზიტორთა რაოდენობის მნიშვნელოვანი ზრდისთვის.

საამისოდ გარკვეული საკითხები ყოველდღიური მუშაობისას თქვენვე უნდა გაითვალისწინოთ და ასევე ზომები მიიღოთ თქვენს ჰოსტინგ პროვაიდერთან (კომპანია, რომლის მეშვეობითაც თქვენი ვებგვერდი გარე სამყაროს, აუდიტორიას უკავშირდება) მიმართებაშიც.

თქვენ მიერ გასათვალისწინებელი საკითხები:

ეს, ზოგადად, ჩვეულებრივ რეჟიმში მუშაობის დროსაც საჭიროა, თუმცა, ვიზიტორთა გაზრდილი რაოდენობის დროს , ორმაგად მნიშვნელოვანია.

Yahoo developer-ის კვლევის თანახმად, ვებგვერდის გახსნისას, დატვირთვების ანუ შენელების 80% HTTP დაკვეთებზე მოდის, რაც იმას ნიშნავს, რომ მომხმარებლის მიერ თქვენი ვებგვერდის მისამართის აკრეფის შემდეგ სერვერიდან მის კომპიუტერში თქვენი ვებგვერდის სხვადასხვა კომპონენტი იტვირთება. ასეთი შეიძლება იყოს ფლეშ ანიმაცია, ფოტოები, ვიდეოები, ვების პროგრამული სკრიპტები, მოდულები და ა.შ.

ყველა კომპონენტის ჩამოტვირთვის შემდეგ, სისტემა ვებგვერდის საერთო რენდერს ახდენს და მომხარებლის კომპიუტერში ის უკვე „აწყობილი“ სახით ჩნდება.

იმისთვის, რომ პირველი ჩამოტვირთვის დაწყებიდან რენდერის დასრულებამდე დროის პერიოდი შევამციროთ, პირველ რიგში, უნდა ვცადოთ, რომ ვებგვერდის დიზაინი მაქსიმალურად სადა და მარტივი იყოს - ნაკლები სკრიპტებით, ფლეშ ანიმაციებით და რთული მოდულებით.

ამ ყველაფრის ოპტიმიზაცია ვებ დეველოპერმა უნდა გააკეთოს, თუმცა ხშირად საიტის მფლობელები მსხვილი მედია კორპორაციების მსგავს დიზაინს ირჩევენ და, იმის გამო, რომ მათი ტექნიკური და ადამიანური რესურსი ბევრად მწირია, საბოლოოდ ვიღებთ იმას, რომ ვიზუალურად მომხიბლავი საიტი ფუნქციურად გაუმართავი რჩება.

ვებგვერდის ოპტიმიზაციისთვის, ვებდეველოპერის გარეშე, თქვენც ბევრი რამის გაკეთება შეგიძლიათ:

- ნუ ატვირთავთ ვებგვერდზე ფოტოებს უსისტემოდ, ერთ საერთო საქაღალდეში. დაახარისხეთ მედია ფაილები დროის და სიტუაციის შესაბამისად და გადაანაწილეთ სხვადასხვა დირექტორიაში. ასე ვებგვერდი ბევრად სწრაფად გაიხსნება და იმუშავებს.
- ნუ ატვირთავთ დიდი ზომის ფოტოებს ვებზე. გახსოვდეთ, ფოტოს დიდი ზომა ყოველთვის არ ნიშნავს კარგ ხარისხს. ფოტოს გამოქვეყნებამდე, მოახდინეთ მისი ოპტიმიზაცია კომპიუტერული ან ონლაინ პროგრამის მეშვეობით.

ონლაინ პლატფორმები ფოტოს დასამუშავებლად:
https://resizeimage.net/
https://compressimage.toolur.com/
https://pdftojpg.me/

ონლაინ პლატფორმა ვიდეო-აუდიოს დასამუშავებლად:
https://bit.ly/3cAiII7

- გრაფიკული გამოსახულება დაიმახსოვრეთ PNG გაფართოებით, ხოლო რეალური ფოტო გამოსახულება JPG გაფართოებით. ვებ ოპტიმიზაციის დროს, გამოიყენეთ კომპრესია და ვებ ოპტიმიზაცია, რასაც კონკრეტული პროგრამის შესაბამის პარამეტრებში მონახავთ.

- ნუ ატვირთავთ ვიდეო რეპორტაჟებს პირდაპირ ვებგვერდზე. ისინი ჯერ ონლაინ ვიდეო დისტრიბუციის საიტებზე - მაგალითად, იუთუბზე ან ვიმეოზე განათავსეთ და შემდეგ, ემბედირებული კოდის მეშვეობით გამოაქვეყნეთ ვებგვერდზე.

საკითხები, რომლებიც ჰოსტინგ პროვაიდერთან უნდა გაიაროთ:

ხშირად, დამწყები ვებმფლობელი ყველაზე იაფფასიან, დაბალბიუჯეტიან გადაწყვეტილებას ირჩევს. არადა ჰოსტინგი ანუ სივრცე, სადაც თქვენი ვებგვერდი განთავსდება, უმნიშვნელოვანესია იმისთვის, რომ შემოსულმა მომხმარებელმა დროულად მიიღოს სასურველი ინფორმაცია. ასევე, თუ ვებ გვერდზე მიმდინარეობს რაიმე ტიპის შეტევა, რესურსებმა უნდა გაუძლონ და თქვენმა მომხმარებელმა უნდა განაგრძოს ინფორმაციის მიღება.

ამიტომ თავი აარიდეთ ე.წ. Shared hosting-ს (საზიარო ჰოსტინგი) და აირჩიეთ VPS სერვისის პაკეტი (ვირტუალური პირადი სერვერი) - ეს ოტიმალური ვერსიაა, თუმცა არსებობს კიდევ უფრო გაუმჯობესებული, მაგრამ შესაბამისად, უფრო ძვირადღირებული ვარიანტიც, ე.წ. Dedicated server-ის (გამოყოფილი სერვერის) სახით.

თვით პაკეტში კი, თქვენი ვებგვერდის დატვირთვებიდან და მასზე გამოქვეყნებული კონტენტის ფორმატიდან გამომდინარე, ყურადღება მიაქციეთ შემდეგ საკითხებს - ვებდეველოპერთან და ჰოსტინგ პროვაიდერთან ერთობლივი კონსულტაციით:

- რესურსების მონიტორინგი (პროცესორი, ოპერატიული მეხსიერება, ქსელი, მყარი დისკი)
- მონიტორინგიდან მიღებული ინფორმაციის საფუძველზე, საჭიროების შემთხვევაში დასამატებელი რესურსების სია და ოდენობა (პროცესორი, ოპერატიული მეხსიერება, ქსელი, მყარი დისკი)
- Firewall-ის არ არსებობის შემთხვევაში, უნდა გაძლიერდეს მონაცემთა ბაზის მონიტორინგი (ქეში, შეერთებების რაოდენობა, მონაცემთა ბაზასთან არალეგალური დაკავშირების მცდელობები, რესურსები)
- Firewall-ის არსებობის შემთხვევაში, უნდა გაძლიერდეს მონიტორინგი, რაც გულისხმობს იმას რომ დროულად მოხდეს რეაგირება ზემოთ ხსენებულ ყველა მოვლენაზე.

მომზადებულია IREX M-TAG პროგრამის ფარგლებში,
დაჩი გრძელიშვილის მიერ

ციფრული უსაფრთხოება

კორონავირუსის პანდემიის პერიოდში მედიასაშუალებებს განსხვავებულ რეჟიმში უწევთ ფუნქციონირება. მათი უმეტესობა დისტანციურ მუშაობაზეა გადასული, რაც კიდევ უფრო ზრდის კიბერუსაფრთხოებასთან დაკავშირებულ რისკებს.

დისტანციური მუშაობისას, ორგანიზაციამ უნდა ააწყოს შიდა ქსელი. ასეთ დროს დგება საკითხი, როგორ უნდა მიწვდეს შიდა რესურსებს მომხმარებელი. ორგანიზაციას შესაძლოა დასჭირდეს დამატებითი ტექნიკის შესყიდვა, მაგალითად, როუტერის, ან სხვა მოწყობილობის, რომელსაც მომხმარებელი შეიძლება დაუკავშირდეს ვირტუალური ქსელის - VPN-ის საშუალებით. ასევე, დგება აუთენტიფიკაციის საკითხი, რომ მომხმარებელს წვდომა მიეცეს ორგანიზაციის შიდა რესურსებზე.

დავით გიორგობიანი გვიზიარებს რჩევებს, თუ როგორ უზრუნველვყოთ ინფორმაციული უსაფრთხოების დაცვა დისტანციური მუშაობისას.

მომხმარებლების ურთიერთობა შიდა რესურსებთან

საჭიროა, ორგანიზაციას გაწერილი ჰქონდეს შიდა რესურსებთან მომხმარებლების ურთიერთობის პოლიტიკა. რესურსების დაცვა უნდა ითვალისწინებდეს:

- პოლიტიკას პაროლების შესახებ;
- პოლიტიკას მომხმარებლების შესახებ;
- პოლიტიკას ელექტრონული ფოსტის მოხმარების შესახებ;
- პოლიტიკას რესურსებთან წვდომის შესახებ.

საჭიროა, პაროლების გენერაცია იყოს რთული ან საშუალო, გააჩნია ორგანიზაციის დამოკიდებულებას, რა მიდგომა აქვს ინფრასტრუქტურის დაცულობაზე. აუცილებლად გაწერილი უნდა იყოს ვის რაზე უნდა ჰქონდეს წვდომა, როგორი მეთოდით უნდა ხდებოდეს მომხმარებლების ორგანიზაციის შიდა ქსელზე წვდომა დისტანციური მუშაობისას.

კავშირის დამყარებისას გასათვალისწინებელია ადგილმდებარეობა. მედიაორგანიზაციებმა უნდა განსაზღვრონ საიდან შეიძლება მოხდეს მომხმარებლის კავშირი შიდა რესურსებთან. ვინაიდან გლობალურ ქსელს არ გააჩნია საზღვრები (იგულისხმება წვდომის წერტილების რაოდენობა), კავშირი შეიძლება იყოს როგორც ლოკალური, ისე გლობალური.

საჭიროა მომხმარებლების მონაცემების დაცვა. ეს ეხება როგორც დისტანციურ მუშაობას, ასევე შიდა ორგანიზაციისა და ვებგვერდის მუშაობას. აქ საფრთხეს წარმოადგენს ის, რომ მომხმარებელი და პაროლი არ უნდა გავიდეს გარეთ. აუცილებლად უნდა დავიცვათ ადმინ პანელთან წვდომა. ორგანიზაციას უნდა ჰქონდეს გაწერილი პოლიტიკა იმის შესახებ, რა პრინციპებით უნდა მოხდეს შიდა რესურსებსა თუ ვებგვერდზე წვდომა.

როდესაც განისაზღვრება როლები, ვის რა როლი აქვს და ვის რაზე უნდა ჰქონდეს წვდომა, შემდეგ დგება საკითხი, როგორ უნდა მიწვდეს შიდა რესურსებს მომხმარებელი, რაც გულისხმობს, ისევ და ისევ განსაზღვრას რა მოწყობილობა არის საჭირო, რომელსაც მომხმარებელი შეიძლება დაუკავშირდეს ვირტუალური ქსელის - VPN-ის საშუალებით.

მნიშვნელოვანი საკითხია მონაცემების შენახვაც. ამ საკითხზეც აუცილებელია ჩამოყალიბებული იყოს გარკვეული პოლიტიკა. არჩევანი უნდა გაკეთდეს რომელ სისტემას ვირჩევთ. გასათვალისწინებელია ისიც, რომ ეს ყველაფერი დაკავშრებულია ფინანსებთან.

აუთენტიფიკაცია

საჭიროა განისაზღვროს, თუ როგორი უნდა იყოს აუთენტიფიკაცია, რომლითაც მომხმარებელს უნდა მიეცეს წვდომა ორგანიზაციის შიდა რესურსებზე.

ერთდონიანი აუთენტიფიკაცია არის ყველაზე დიდი პრობლემა. საკმარისია კიბერ შეტევა განხორციელდეს, არაკეთილსინდისიერ მომხმარებელს უკვე აქვს პირდაპირი წვდომა მედიაორგანიზაციის შიდა რესურსებზე.

თუ ორგანიზაციას მაინც ერთდონიანი აუტენტიფიკაცია აქვს, მან უნდა უზრუნველყოს მომხმარებლისა და პაროლის დროული ცვლილება, ერთჯერადი პაროლების გამოყენება.

რეკომენდებულია, ორგანიზაციამ გაითვალისწინოს მრავალდონიანი აუთენტიფიკაცია. შესაძლოა, ეს იყოს უბრალოდ მომხმარებლისა და პაროლის შეყვანა, მაგრამ როგორც კი პირველი აუთენტიფიკაცია მოხდება, მას უნდა დაეწიოს მეორე იდენტიფიცირების საშუალება. მაგალითად, მეილით ან მოკლე ტექსტური შეტყობინებით მიუვიდეს კოდი. შეიძლება, ეს იყოს ერთჯერადი პაროლებიც. ამ უკანასკნელ შემთხვევაში, გასათვალისწინებელია პაროლის მოქმედების ვადა.

ვებრესურსების დაცვა

აუცილებელია გარე რესურსების სწორად აწყობა და დაცვა. ვებგვერდი შეიძლება აუთსორსზე იყოს გატანილი, მაგრამ არ უნდა ვიფიქროთ, რომ ის სრულად არის დაცული. თუ ვებგვერდი აუთსორსზეა გატანილი, ასეთ დროს მედიაორგანიზაციას შეუძლია მოსთხოვოს აუთსორს კომპანიას აუთენტიფიკაციის მეთოდების დაცვა, კავშირი ადმინისტრირების პანელთან, საიდანაც შეიძლება მოხდეს კონტენტის შეცვლა, წაშლა და ა.შ. რამაც, შესაძლოა, დიდი ზიანი მიაყენოს ორგანიზაციას.

საჭიროა, ვებგვერდის ადმინ პანელზე გაწერილი იყოს, თუ ვის შეუძლია ჰქონდეს წვდომა, საიდან და როგორ.

დღეს საკმაოდ გაზრდილია ვებგვერდებზე ვიზიტორთა რაოდენობა. ამიტომ, აუცილებელია, ჰოსტერთან სამუშაოდ გაიწეროს გარკვეული პოლიტიკა. ასევე, გაიზარდა ალბათობა და რისკი, რომ ინფორმაციასთან წვდომის გამო, შეიძლება, მოხდეს სხვადასხვა ტიპის შეტევები ვებგვერდზე და ამით მოხდეს მედიასაშუალების ინფორმაციის გავრცელების დაბრკოლება. მაგალითად, თუ ჰოსტერების სერვერების გატეხვა მოხდა, მედიასაშუალებების მუშაობაც გაჩერდება.

რა უნდა გაითვალისწინოს მომხმარებელმა

გასათვალისწინებელია, რომ დისტანციურ მუშაობაზე გადასვლით, ინტერესის ობიექტი ხდება არა ორგანიზაცია, არამედ ის ადამიანი, რომელიც დასაქმებულია ამ ორგანიზაციაში. თანამშრომელი უკვე წარმოადგენს სუსტ წერტილს, თუ არაკეთილსინდისიერმა მომხმარებელმა შეძლო მისი პერსონალური კომპიუტერის მართვის მოპოვება.

ზოგჯერ ორგანიზაცია თანამშრომელს აძლევს ორგანიზაციის შიდა ტექნიკას, მაგრამ ეს არ ნიშნავს იმას, რომ იგი სრულადაა დაცული. ასეთ დროს, გათვალისწინებულია სისტემური პარამეტრები, რომლითაც ბევრი უფლებაა შეზღუდული (შეზღუდვები დამოკიდებულია ორგანიზაციის პოლიტიკაზე). ამ შემთხვევაში, მთავარია, რომ სამსახურის ტექნიკაზე წვდომის შესაძლებლობა არავის მიეცეს.

დისტანციური მუშაობისას აუცილებელია გათვალისწინებული იყოს, რომ თანამშრომელს:

- კომპიუტერზე ჰქონდეს ანტივირუსი;
- ჰქონდეს გამართული ოპერაციული სისტემა;
- იცავდეს პაროლებს პერსონალურ სივრცეში;

- გაითვალისწინოს ინტერნეტის ხარისხი და ინტერნეტ პაკეტის სერვისები.

თანამშრომლის IP მისამართი, შესაძლებელია, იყოს სტატიკური, ან დინამიური. ორივე შემთხვევას აქვს თავისი პლიუსები და მინუსები. აუცილებელია შეთანხმება ინტერნეტ პროვაიდერებს, მომხმარებლებსა და მედიაორგანიზაციებს შორის, თუ რომელი ტიპის მისამართის გამოყენება იქნება შესაძლებელი. სტატიკური მისამართის შემთხვევაში მომხმარებელი ხდება შედარებით მარტივი სამიზნე, თუმცა, ორგანიზაციის პოლიტიკიდან გამომდინარე, შედარებით მარტივია დაცვის სისტემების გამოყენება. დინამიური მისამართის (შეიძლება შეიცვალოს პოლიტიკიდან გამომდინარე) გამოყენების დროს, დაცვის მექანიზმების გამოყენება უფრო საყურადღებოა, რადგან ამ შემთხვევაში ვერ გამოვიყენებთ კონკრეტული მისამართის მონიტორინგს.

მომხმარებლებმა უნდა გაითვალისწინონ მონაცემების დაკარგვის საფრთხე და იზრუნონ, რომ არავინ მოიპაროს მათი მონაცემები. ინფორმაციის მოპარვის საშუალებები ბევრია, მათ შორის, ფიშინგი, ბრუთფორსი, ქეილოგერი, მალვეარი და სხვა.

ინფორმაციის წაღება შიეძლება ელექტრონულ ფოსტაზე გამოგზავნილი არაკეთილსინდისიერი ბმულითაც, რომელზე გადასვლის შემდეგ, მომხმარებლის კომპიუტერში შეიძლება აღმოჩნდეს პროგრამა, რომელიც კომპიუტერში აკრეფილ მონაცემს, მათ შორის საბანკო ბარათის მონაცემებს მოიპარავს.

კომპიუტერის არასათანადო დაცვის შემთხვევაში, მაგალითად, როდესაც არ გვაქვს დაყენებული ანტივირუსი, ფაიერვოლი, არ ვაქცევთ ყურადღებას იუზერის და პაროლის შეყვანას კომპიუტერზე, შესაძლებელია, ჩაიწეროს აბსოლუტურად ყველა მონაცემი, რომელიც შეგვყავს კომპიუტერში და გაიგზავნოს არაკეთილსინდისიერ მომხმარებელთან, რაც პრობლემას წარმოადგენს როგორც მომხმარებლისთვის, ასევე ორგანიზაციისთვის.

ფაიერვოლი უზრუნველყოფს გარე რესურსებიდან შიდა რესურსებზე წვდომის შეზღუდვას. ეს არის დაცვის საშუალება. ასევე, შეგვიძლია, დავაყენოთ პროგრამული ფაიერვოლები (access manager; privilege user manager; identity manager) და სხვა.

დიდი ყურადღება უნდა მივაქციოთ ფაიერვოლის არსებობას. აგრეთვე, უნდა გავითვალისწინოთ, რომ არსებობს IPS-ები - შემოღწევის დროს პრევენცია. აუცილებელია მოწყობილობების პროგრამული განახლებები. შეტევების რაოდენობა იმდენად დიდია, რომ ყოველდღიურად ხდება საიტების შავი სიის (სარეპუტაციო ბაზები) განახლება. ეს განახლებები უნდა მიმდინარეობდეს ნებისმიერ ორგანიზაციაში, აუთსორსი იქნება თუ ჩვეულებრივი.

აუცილებელია, რომ არ დავტოვით ღიად არც ერთი სესია, რომელსაც კავშირი აქვს სერვერთან. სერვერი ან სერვისი გარკვეული დროის მერე უნდა წყვეტდეს კავშირს ავტომატურად.

გასათვალისწინებელია სოციალური ქსელების გამოყენების საკითხიც. შესაძლოა, მედიაორგანიზაციას ჰქონდეს პოლიტიკა და დაბლოკილი იყოს სოციალური ქსელები, მაშინ, როდესაც დისტანციური მუშაობისას, სახლიდან თავისუფლად შეგვიძლია გამოვიყენოთ ისინი. არაკეთილსინდისიერმა მომხმარებლებმა შეიძლება მოიპოვონ წვდომა თანამშრომლის კომპიუტერზე, თუნდაც სოციალური ქსელის გატეხვის გზით. ასეთ დროს, დაცვის ერთ-ერთი საშუალება მულტი აუთენტიფიკაციაა. ლოგებით შეგვიძლია შევამოწმოთ, ვინ შემოვიდა, ან ვინ ცდილობდა შემოსვლას პერსონალურ გვერდზე.

ციფრული უსაფრთხოების საკითხებზე ჟურნალისტებისთვის რეკომენდაციები გამოქვეყნებული აქვს ჟურნალისტთა უფლებების დამცველ საერთაშორისო ორგანიზაცია CPJ-ს. როგორც ორგანიზაცია აღნიშნავს, COVID-19-ის გაშუქებასთან დაკავშირებით, შესაძლოა, ჟურნალისტების ონლაინ უსაფრთხოებას შეექმნას საფრთხე.

გთავაზობთ CPJ-ის მიერ მომზადებულ რეკომენდაციებს:

- გაითვალისწინეთ, რომ COVID-19-ის გავრცელების მონიტორინგის მიზნით, მთავრობები და ტექნოლოგიური კომპანიები დაზვერვის გზას მიმართავენ. Citizen Lab-ის ინფორმაციით, ეს მოიცავს NSO Group-საც, რომელმაც შექმნა სათვალთვალო პროგრამა Pegasus. პროგრამა შეიძლება გამოყენებული იქნას ჟურნალისტების წინააღმდეგ.
- შეჩერდით და დაფიქრდით, სანამ ბმულზე გადახვალთ ან COVID-19-ის შესახებ ინფორმაციის შემცველ დოკუმენტებს გადმოიწერთ. კრიმინალები შექმნილ სიტუაციას იყენებენ კონკრეტულ პირებსა და ორგანიზაციებზე ე.წ ფიშინგისთვის, რამაც, შესაძლოა, თქვენს მოწყობილობებზე ვირუსული პროგრამების დაინსტალირება გამოიწვიოს.
- სიფრთხილე გამოიჩინეთ სოციალურ მედიასა და მიმოწერის აპლიკაციებში COVID-19-თან დაკავშირებულ ბმულებზე გადასვლისას. ზოგიერთმა ბმულმა, შესაძლოა, გადაგიყვანოთ ვებგვერდებზე, რომლებიც თქვენს მოწყობილობებს დაავირუსებს. ყოველთვის გახსოვდეთ მავნე აპლიკაციების შესახებ, რომლებიც შანტაჟის მიზნით გამოიყენება, მაგალითად - COVID-19 Tracker.

- ცნობილია, რომ რუკები, რომლებიც სანდო წყაროებზე, მაგალითად, WHO-ზე დაყრდნობით, კორონავირუსის განახლებულ ინფორმაციას ასახავს, შესაძლოა, შეიცავდეს ვირუსს, რომელიც პაროლების მოსაპარად გამოიყენება.
- გაითვალისწინეთ, სახელმწიფოს მიერ დაფინანსებული დეზინფორმაციაც. ამის შესახებ The Guardian და BBC-იც წერენ. ასევე, დეზინფორმაციაზე ყურადღებას ამახვილებს WHO. მითების შესახებ ინფორმაცია ხელმისაწვდომია ჯანდაცვის მსოფლიო ორგანიზაციის ვებგვერდზე.
- ფრთხილად იყავით, მიმოწერის აპლიკაციებში კორონავირუსზე გავრცელებულ ინფორმაციებთან დაკავშირებით. ისინი შესაძლოა ყალბ ამბებს წარმოადგენდნენ.
- გაითვალისწინეთ, რომ Facebook-ზე COVID-19-ის კონტენტს მოდერატორობას არა ადამიანები, არამედ ხელოვნური ინტელექტი უწევს, რის გამოც ვირუსის შესახებ რეალურ ფაქტებზე დაფუძნებული მასალების შეცდომით წაშლის ფაქტი უკვე დაფიქსირდა.
- წაიკითხეთ ონლაინ კონფერენციებისა და კონფიდენციალურობის საკითხები, რათა იცოდეთ როგორ იყენებენ ეს სერვისები თქვენს მონაცემებს, რაზე აქვთ მათ წვდომა და რამდენად დაცულები არიან. გაითვალისწინეთ, რომ სახლიდან მომუშავეთა რიცხვის გაზრდასთან ერთად, ასეთი სერვისები ჰაკერების სამიზნეებად იქცა.