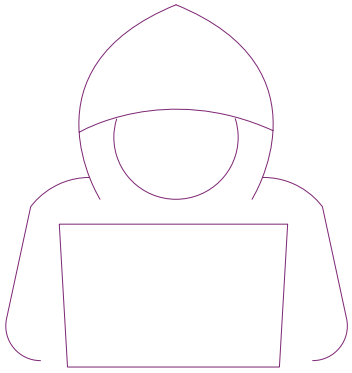
UK Government

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

კიბერმედეგობა ქალთა უფლებების დამცველი ორგანიზაციებისთვის

გზამკვლევი ქართველი აქტივისტების, მშვიდობის მშენებლებისა და უფლებადამცველებისთვის



ავტორი: **ჯენიფერ კანაანი**
რედაქტორი: **დანიელა პელედი**
ქართული თარგმანი: **ნინო ოძელაშვილი**
დიზაინი შექმნილია: **Humble Bee Design**-ის მიერ
დიზაინი ქართულ ენაზე ადაპტირებულია: **ნუგზარ არჩემაშვილი**

კიბერმედეგობა ქალთა უფლებების დამცველი ორგანიზაციებისთვის

გზამკვლევი ქართველი აქტივისტების, მშვიდობის მშენებლებისა და უფლებადამცველებისთვის

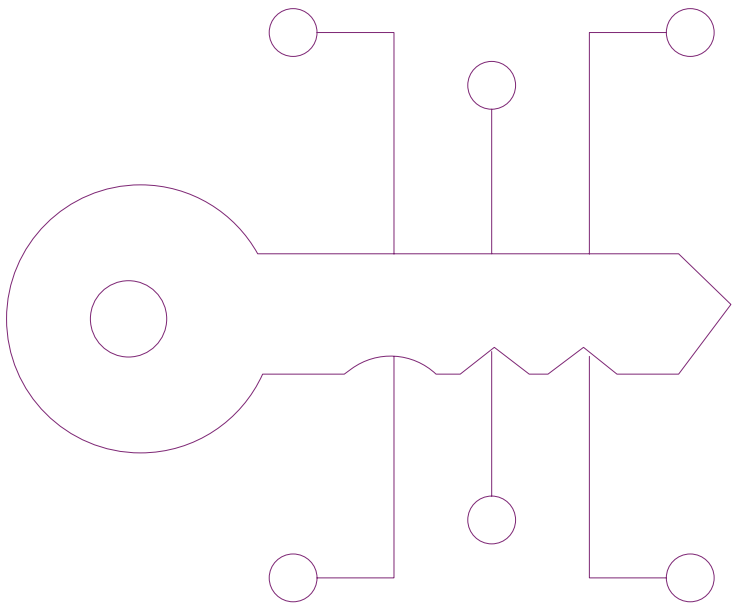
გზამკვლევი მომზადდა „მედეგობის გაძლიერება აღმოსავლეთ სამეზობლოში“ (BREN) პროექტის ფარგლებში, რომელიც გაერთიანებული სამეფოს საგარეო თანამეგობრობისა და განვითარების ოფისის (FCDO) მხარდაჭერით განხორციელდა. პუბლიკაციაში მოხსენიებული მოსაზრებები, აღმოჩენები და დასკვნები ეკუთვნის ავტორებს და ცალსახად არ გამოხატავს გაერთიანებული სამეფოს მთავრობის შეხედულებებს.

BREN-ის პროექტი, რომელიც „მშვიდობის მშენებელ ქალთა გლობალურ ქსელთან“ (GNWP) პარტნიორობით ხორციელდება, შემუშავებულია სსო-ების მდგრადობის გასაძლიერებლად სამხრეთ კავკასიასა და მოლდოვაში, ადამიანის უსაფრთხოების, მშვიდობისა და სტაბილურობის ხელშეწყობის მიზნით. პროექტის განსაკუთრებული ფოკუსი მიმართულია ქალებსა და სხვა მარგინალიზებულ ჯგუფებზე.

„ომისა და მშვიდობის გაშუქების ინსტიტუტი“ (IWPR) მხარს უჭერს ადგილობრივ ხმებს, რათა მათ განახორციელონ ცვლილებები კონფლიქტის, კრიზისისა და გარდამავალი ეკონომიკის ქვეყნებში. იქ, სადაც გამწვავებულია სიძულვილის ენა და პროპაგანდა, ხოლო ჟურნალისტები და სამოქალაქო აქტივისტები თავდასხმის ქვეშ არიან, IWPR-ი სანდო ინფორმაციის გავრცელებასა და საჯარო დებატებს უწყობს ხელს, რაც მნიშვნელოვან პოზიტიურ გავლენას ახდენს ვითარებაზე.

ამ გზამკვლევში მოწოდებული ინფორმაცია არ წარმოადგენს და არ არის გამიზნული წარმოადგენდეს კიბერუსაფრთხოების შესახებ რჩევებს; სანაცვლოდ, იგი განკუთვნილია მხოლოდ ზოგადი საინფორმაციო მიზნებისთვის გამოსაყენებლად.

ორგანიზაციებისთვის გადამწყვეტი მნიშვნელობა აქვს კიბერუსაფრთხოების მრჩეველთან, კონსულტანტთან, ან სულ მცირე, IT ექსპერტთან თანამშრომლობას, რომელიც დაეხმარება მათ კიბერგარემოს გაძლიერებაში და უზრუნველყოფს დახმარებას, კონსულტაციას და სწრაფ რეაგირებას კიბერთავდასხმის ან სხვა კიბერსაფრთხეების გამოვლენის შემთხვევაში.



INSTITUTE FOR WAR & PEACE REPORTING

IWPR

ჯენიფერ კანაანის შესახებ:
ჯენიფერ კანაანი „ომისა და მშვიდობის გაშუქების ინსტიტუტის“ (IWPR) პროგრამის, „მედეგობის გაძლიერება აღმოსავლეთ სამეზობლოში“ (BREN) რეგიონული კომუნიკაციების მენეჯერია. ციფრული კომუნიკაციისა და ადვოკატირების ექსპერტი, ჯენიფერი 2016 წლიდან თანამშრომლობს IWPR-თან და ჩართულია მრავალფეროვან პროექტებში. მათ შორის, ინოვაციურ პროექტში „კიბერ არაბები“ (Cyber Arabs), IWPR-ის ყოვლისმომცველი არაბულენოვანი კიბერუსაფრთხოების რესურსების ვებგვერდი და ციფრული ადვოკატირების სახელმძღვანელო Etihad-ისთვის, პროექტი, რომელიც მხარს უჭერს LGBTQI ორგანიზაციებს შუა აღმოსავლეთისა და ჩრდილოეთ აფრიკის რეგიონში.

დანიელა პელედის შესახებ:
დანიელა პელედი IWPR-ის აღმასრულებელი რედაქტორია, რომელიც ზედამხედველობას უწევს ყველა სახის სარედაქციო მასალის წარმოებას. ჟურნალისტმა და რედაქტორმა, რომელსაც 20 წელზე მეტი გამოცდილება აქვს საგარეო საქმეთა გაშუქების სფეროში, ასევე შეიმუშავა და განახორციელა ჟურნალისტიკის ტრენინგი IWPR-ის საქმიანობის სხვადასხვა რეგიონებში, მათ შორის ავღანეთში, ერაყსა და თურქეთში.

მადლობა Toro-ს და „მშვიდობის მშენებელ ქალთა გლობალურ ქსელს“ (GNWP)
კიბერუსაფრთხოების ექსპერტები: სამველ მარტიროსიანი, არტურ პაპიანი, დავით ღონღაძე და ვლად მაზურაკი.

gnwp Global Network of Women Peacebuilders

კიბერუსაფრთხოების გარემო საქართველოში: გენდერული ანალიზი

ევროპისა და აზიის გზაჯვარედინზე მყოფი საქართველოს პოლიტიკური რელიეფი ისტორიული სირთულეებით არის ფორმირებული. ქვეყანა უსაფრთხოების დილემის წინაშე დგას, რომელიც რუსეთთან მისი რთული ურთიერთობებით არის გამწვავებული. დასავლეთთან მჭიდრო კავშირების მომხრეთა და პრორუსული მიდრეკილებების მქონე პირებს შორის უთანხმოება გამძაფრებას განაგრძობს, რაც საქართველოს პოლიტიკურ დინამიკაში კიდევ უფრო მეტ ფენებს აჩენს. (1) უკრაინის ომმა გააღვივა დაძაბულობა და 2008 წელს, საქართველოს ტერიტორიაზე რუსეთის შემოჭრის მოგონებები გამოაღვიძა. ამავდროულად, აფხაზეთსა და სამხრეთ ოსეთში რუსეთის გავლენის სიმტკიცის აღდგენას შეუწყო ხელი. (2)

გეოპოლიტიკურ ფაქტორებთან გადახლართული კიბერუსაფრთხოების გარემო რუსეთს მნიშვნელოვან საფრთხედ წარმოაჩენს, რომელიც ჰაკერულ და დეზინფორმაციის კამპანიებშია ჩართული. 2023 წლის მარტში, საქართველოს მთავრობის მიერ რუსული სტილის „უცხოელი აგენტების რეგისტრაციის შესახებ“ კანონპროექტის მიღებას ფართომასშტაბიანი პროტესტი მოჰყვა. კანონპროექტის კრიტიკოსების მტკიცებით, ეს იყო სამოქალაქო საზოგადოების ჩახშობისა და თავისუფლების შეზღუდვის წარუმატებელი მცდელობა. (3, 4, 5)

კანონპროექტის გაწვევის მიუხედავად, გამუდმებით მტრული გარემო ნარჩუნდება სამოქალაქო საზოგადოების ორგანიზაციების, უფლებადამცველებისა და აქტივისტების მიმართ. (6)

კიბერუსაფრთხოების გარემო

ბოლო წლებში, საქართველო სხვადასხვა კიბერშეტევების წინაშე აღმოჩნდა. მათ შორის, დომინანტური საფრთხე რუსეთის მაღალი დონის მუდმივ საფრთხეებს (APTs) მიეკუთვნება. (7, 8)

ქვემოთ მოცემულია შემჩნეული კიბერშეტევების რამდენიმე გავრცელებული ტიპი:

- **სერვისზე წვდომის შეზღუდვის (DoS) შეტევა:** თავდასხმა მიზნად ისახავს სერვისებზე ხელმისაწვდომობის შეფერხებას, რაც დისკომფორტს და პოტენციურ ფინანსურ ზარალს იწვევს.
- **ვებ აპლიკაციის იერსახის ცვლილება (Defacement):** მსგავსი კიბერშეტევები, რომლებიც 2019 წელს, საქართველოზე მასიური კიბერშეტევის დროს დაფიქსირდა, ცხადყოფს ვებ აპლიკაციების დაუცველობას. (9)
- **მავნე პროგრამული უზრუნველყოფის (Malware) შეტევები:** მავნე პროგრამული უზრუნველყოფა, როგორიცაა გამოსასყიდის (ransomware) ან ჯაშუშური (spyware) პროგრამები, მნიშვნელოვან საფრთხეს წარმოადგენს საქართველოს კიბერუსაფრთხოებისთვის და პოტენციური საფრთხის წინაშე აყენებს სენსიტიურ ინფორმაციასა და სისტემებს.
- **ფიშინგი (Phishing):** სოციალური ინჟინერიის ისეთი ტექნიკები, როგორიცაა „ფიშინგი“ ინდივიდების მოტყუების გზით, მათ სისტემებზე უნებართვო წვდომის მოსაპოვებლად გამოიყენება.
- კიბერ თაღლითობა და ფულის გათეთრება: საქართველოს კიბერდანაშაულების საგამოძიებო ჯგუფი აქტიურად მუშაობს ისეთ კიბერ საფრთხეებზე, რომლებიც თაღლითობასა და ფულის გათეთრებასთან არის დაკავშირებული. საგამოძიებო ჯგუფი ცნობიერების ამაღლების და თავდაცვის აუცილებელი ზომების მიღების მნიშვნელობას უსვამს ხაზს. (10)

სამოქალაქო საზოგადოება და კიბერ საფრთხეები

საქართველოს სამოქალაქო საზოგადოება, ქვეყნის რთული გეოპოლიტიკური ვითარებების გათვალისწინებით, მნიშვნელოვან კიბერ საფრთხეებს უპირისპირდება. ამ კონტექსტში, ეროვნული უსაფრთხოების საბჭომ კიბერუსაფრთხოების ყოვლისმომცველი სტრატეგია შეიმუშავა 2021-2024 წლებისთვის, რომელიც კიბერ საფრთხეების მიმართ ქვეყნის მდგრადობის გაძლიერებას ისახავს მიზნად. მთავრობამ მხარი დაუჭირა საქართველოს მე-3 ეროვნულ კიბერუსაფრთხოების სტრატეგიას 2021-2024 წლებისთვის. (11)

ადამიანის უფლებების, დემოკრატიისა და სამოქალაქო ჩართულობის დამცველი სამოქალაქო საზოგადოების ორგანიზაციების როლი არსებითია საქართველოსთვის. მათი კრიტიკული ფუნქციების მიუხედავად, ეს ორგანიზაციები კიბერ საფრთხეების მიმართ არიან მიდრეკილები. სამოქალაქო საზოგადოების ციფრული უსაფრთხოების რისკებს ზრდის დინამიკური კიბერ გარემო, გამძაფრებული რუსეთის, როგორც მნიშვნელოვანი საფრთხის იდენტიფიცირებული როლით, რომელიც კიბერჰაკერულ და დეზინფორმაციულ კამპანიებს აწარმოებს.

დამატებით, უსაფრთხოების სექტორზე ზედამხედველობის სამოქმედო გეგმა მკაცრი განხილვის ქვეშ იმყოფება, რომელიც ევროკავშირის მოთხოვნების შეუსრულებლობის გამო გააკრიტიკეს. დემოკრატიის კვლევის ინსტიტუტმა (DRI) აღნიშნა, რომ მთავრობის სამოქმედო გეგმის ის ნაწილი, რომელიც უსაფრთხოების სექტორზე საპარლამენტო კონტროლის გაუმჯობესებას ეხება, ამ მიმართულებით გასატარებელ ღონისძიებებს მოკლებულია. (12)

გენდერული ანალიზი კიბერ საფრთხეებში

კიბერ საფრთხეები ფართოდ გავრცელებული პრობლემის სახით აღმოცენდა, რომელიც მთელი მსოფლიოს მასშტაბით ახდენს ზემოქმედებას ინდივიდებზე. სამწუხაროდ, ქალებს, რომლებიც უნიკალური გამოწვევებისა და დაუცველობის წინაშე დგანან, ხშირად უწევთ ამ საფრთხეების სიმძიმის ტარება. მსოფლიოში, ქალთა მიმართ კიბერძალადობა მწვავე პრობლემად რჩება, რომელიც კიბერ შევიწროების, შურისძიების პორნოს და ძალადობრივი კონოტაციის მქონე ონლაინ თავდასხმების (13 14, 15) ფორმებს მოიცავს. მსგავსი თავდასხმები ხშირად გადაიზრდება შემზარავ საფრთხეებში, რაც ბოსნია და ჰერცეგოვინაში ქალ ჟურნალისტებზე სიკვდილის მუქარით გამოწვეულ ინციდენტებშია ასახული (16).

2023 წელს, GNWP-ის მიერ ჩატარებული კვლევა „გენდერი და ადამიანის უფლებები ეროვნულ დონეზე კიბერუსაფრთხოების მიდგომებში“ ხაზს უსვამს გენდერული პერსპექტივის ჩართვის მნიშვნელობას პოლიტიკის შემუშავების პროცესში (17). ეს მოდგომები ადასტურებს, რომ ქალთა უფლებების დამცველი ორგანიზაციები უნიკალური გამოწვევების წინაშე დგანან და განსაკუთრებულ ანალიზს და რეკომენდაციებს საჭიროებენ.

GNWP-ს ანგარიშის თანახმად, კიბერუსაფრთხოების გენდერულ ჭრილში განხილვის უპირატესობები მოიცავს:

1. იმის აღიარებას, რომ ქალები და სხვა მარგინალიზებული ჯგუფები განსხვავებულად იყენებენ ინტერნეტს და არაპროპორციულად ზარალდებიან კიბერშეტევებით. ხშირად, მათი სპეციფიკური საჭიროებები და ჩართულობა კიბერუსაფრთხოების პოლიტიკის შემუშავებისა და ტექნოლოგიების განვითარების პროცესებში უგულებელყოფილი რჩება.
2. ქალებისა და სხვა მარგინალიზებული ჯგუფებისთვის კიბერუსაფრთხოების დებულებებზე ხელმისაწვდომობის გაუმჯობესებას, საგანგებო სიტუაციებზე რეაგირებისა და სამართლებრივი დაცვის საშუალებებზე ხელმისაწვდომობის კუთხით არსებული შეზღუდვების აღმოფხვრის მიზნით, რაც არსებული დისკრიმინაციული საზოგადოებრივი სტრუქტურების შედეგად ჩამოყალიბდა.
3. კიბერუსაფრთხოების პოლიტიკაში არსებული ხარვეზების აღმოფხვრას გენდერული პერსპექტივის ჩართვის გზით, ადამიანებზე ორიენტირებული და გენდერულად მგრძნობიარე მიდგომის ხაზგასმით.

კიბერშეტევები უდავო გავლენას ახდენს ქალებზე საქართველოში, რაც კიბერბულინგის, კიბერ-ადევნების და სექსუალური მიზნებისთვის დაყოლიების ფორმებში გამოიხატება. მსგავსი თავდასხმები ზღუდავს ქალთა გამოხატვის თავისუფლებას და დამანგრეველად მოქმედებს მათ თვითრწმენასა და თვითშეფასებაზე.

2017 წელს, საქართველოს სტატისტიკის ეროვნულ სამსახურთან (საქსტატი) თანამშრომლობით, UN Women-მა, 2009 წლის შემდეგ, პირველი კვლევა ჩაატარა ქვეყნის მასშტაბით ქალთა მიმართ ძალადობის შესახებ. კვლევამ საგანგაშო მონაცემები გამოავლინა სექსუალური შევიწროებისა და ადევნების მხრივ. ცხოვრების მანძილზე, ყოველი მეხუთე ქალი გამხდარა მსგავსი შემთხვევის მსხვერპლი. მათ შორის, ინციდენტების 70 პროცენტს ადგილი ჰქონდა საჯარო სივრცეში (18).

ზემოხსენებულ დასკვნებს გამოეხმაურა გენდერული თანასწორობის მუდმივმოქმედი საპარლამენტო საბჭო და საკანონმდებლო ცვლილებები წამოიწყო, რომლებიც სექსუალური შევიწროების პრევენციასა და მათზე რეაგირებას ისახავს მიზნად.

2019 წლის მაისში ამოქმედდა ყოვლისმომცველი კანონი სექსუალური შევიწროების შესახებ, რომელიც არეგულირებს სექსუალური შევიწროების ინციდენტებს როგორც საჯარო, ასევე სამუშაო სივრცეებში. დაწესდა ჯარიმები მათთვის, ვისაც დაუდგინდება არასასურველი სექსუალური ქმედების დანაშაული (19).

გლობალურად, ქალებისთვის უსაფრთხო ციფრული გარემოს შესაქმნელად, კიბერუსაფრთხოებისა და ქალთა უფლებების გადაკვეთა მუდმივ ყურადღებას და მოქმედებას მოითხოვს. გენდერზე ორიენტირებული მიმდინარე კვლევები და კიბერუსაფრთხოების ინიციატივები გადამწყვეტია ქართულ კონტექსტში ქალებზე კონკრეტული გავლენის გასააზრებლად.

მართლა სამიზნე ვარ?

დიახ! სინამდვილეში, ნებისმიერი შეიძლება გახდეს კიბერშეტევის სამიზნე!

მიზანი შიშის ან პანიკის გამოწვევა არაა. თუმცა, კიბერ საფრთხისა და დანაშაულებრივი ქმედებების სრულად გასააზრებლად, მნიშვნელოვანია პრაგმატულად ფიქრი. ამ რეალობის გააზრება არა მხოლოდ გამოწვევებთან გამკლავებაში, არამედ თქვენი კოლეგების, ბენეფიციარებისა და საკუთარი საქმის დაცვაში დაგეხმარებათ.

განურჩევლად იმისა, თუ რომელ მათგანს წარმოადგენთ საქართველოში - ჰუმანისტს, აქტივისტს თუ ქალთა უფლებების დამცველს, თქვენი მთავარი მიზანი ცვლილებების ქომაგობა, საკანონმდებლო საქმიანობაში გენდერული პერსპექტივების ლობირება და საზოგადოებრივი ცნობიერების ამაღლებაა.

შესაძლებელია, კიბერ საფრთხეები თქვენი ძირითადი განხილვის საგანი არ იყოს და უდავოდ, თქვენგან არც არავინ ელის, რომ კიბერ დამნაშავესავით მიუდგებით საკითხებს. და მაინც, გენდერული პერსპექტივების პოლიტიკურ და სამართლებრივ საკითხებში ჩართვის მსგავსად, თანამედროვე სამყაროში, კიბერ ცნობიერების ინტეგრირება არსებითია ყველა სახის საქმიანობაში.

> საკუთარი თავის, კოლეგებისა და ორგანიზაციის დაცვით მხოლოდ ინფორმაციას არ იცავთ, არამედ უფრთხილდებით საზოგადოებაზე იმ პოზიტიურ გავლენას, რომელიც გაქვთ და გექნებათ მომავალშიც.

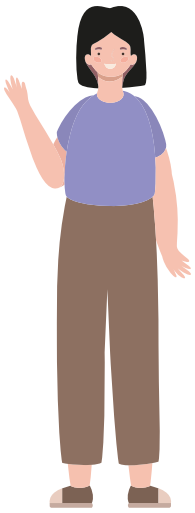
გაიცანით ნინო და სალომე

ნინო, გულანთებული ადამიანის უფლებების დამცველი, თავის ცხოვრებას პოზიტიური ცვლილებების წახალისებას უძღვნის. მისი სამუშაო დღე ქალების უფლებების დამცველ ლოკალურ ორგანიზაციებთან შეხვედრებს, გენდერული თანასწორობის პროგრესის სტრატეგიის შემუშავებასა და ახალგაზრდა აქტივისტების მენტორობას მოიცავს. ის არაერთ საღამოს უთმობს საზოგადოების ჩართულობის პროგრამებს, სადაც ქალებს შთამაგონებელ ამბებს უზიარებს. ნინოს ყოველდღიურობა ადვოკატირებას, სწავლებას და სამოტივაციო საუბრებს მოიცავს.

სალომე, თავდადებული მშვიდობის მშენებელი და საზოგადოების ლიდერი, სამოქალაქო აქტივიზმის ინიციატივებზეა ფოკუსირებული და აქტიურად არის ჩართული დიალოგისა და ურთიერთგაგების წახალისებაში. ხშირად უძღვება სამუშაო შეხვედრებს და მართავს სამშვიდობო ღონისძიებებს, რაც საზოგადოების მრავალფეროვან ჯგუფებს შორის ერთობის ჩამოყალიბებას უწყობს ხელს. სალომეს საქმიანობა კონფლიქტების გადაწყვეტის თემაზე ორგანიზებულ საღამოს დისკუსიებზეც ვრცელდება, რომლებიც საზოგადოების წევრების ჩართულობით იმართება. მისი სამუშაო დღე სავსეა შეხვედრებით, სემინარებით და თანამშრომლობითი ინიციატივებით, რომლებიც მშვიდობიანი და ინკლუზიური სოციუმის შექმნას ისახავს მიზნად.

ნინო

ქალთა უფლებების დამცველი

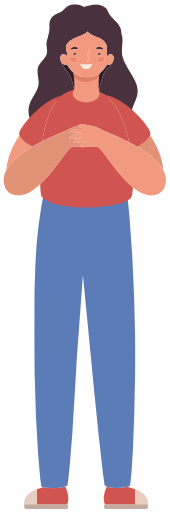


სამუშაო გამოცდილება: ნინო საქართველოში ადამიანის უფლებების ცნობილი დამცველია, რომელიც საკუთარ კარიერას გენდერულ თანასწორობასა და სამართლიანობას უძღვნის. მისი საქმიანობა პოსტკონფლიქტურ რეგიონებში ქალების გაძლიერებისკენ არის მიმართული, რაც მდგრადი მშვიდობის დამყარებას უწყობს ხელს.

ცხოვრების სტილი: ნინო აქტიურადაა ჩართული საზოგადოების გამაძლიერებელ ინიციატივებსა და სამშვიდობო მოლაპარაკებებში. ინკლუზიურობისა და სოციალური სამართლიანობის მიმართ ერთგულებამ, ის ქალთა უფლებების დამცველთა შორის პატივსაცემ ფიგურად აქცია.

სალომე

მშვიდობის მშენებელი და საზოგადოების ლიდერი



სამუშაოს აღწერა: სალომე თავდადებული მშვიდობის მშენებელია, რომელიც აქტიურად მონაწილეობს ომის, ძალადობისა და სოციალური უთანასწორობის წინააღმდეგ მიმართულ ინიციატივებში. ის საკუთარი სამშვიდობო ინიციატივის თანადამფუძნებელია, რომელიც დიალოგისა და ურთიერთგაგების ხელშეწყობას ისახავს მიზნად.

ცხოვრების სტილი: სალომე სათემო სამუშაო შეხვედრებს უძღვება, სადაც სამშვიდობო პროცესებში ქალთა ჩართულობის მნიშვნელობას უსვამს ხაზს. მისი სამოქალაქო ჩართულობის ინიციატივები მშვიდობის შენებისა და ქალთა უფლებების თანაკვეთის ნათელი მაგალითია.

რატომ ირჩევენ სამიზნედ აქტივისტებს, მშვიდობის მშენებლებსა და საზოგადოების ლიდერებს?

კიბერ დამნაშავეები აღნიშნული როლების წარმომადგენლებს საზოგადოებაზე მათი გავლენის გამო ირჩევენ. სწორედ პოზიტიური ცვლილებებისკენ მიმართული მცდელობები აქცევს მათ საწინააღმდეგო სურვილების მქონეთაგან პოტენციური საფრთხის სამიზნედ. მათი სამუშაოს სპეციფიკიდან გამომდინარე, ხშირად აქვთ წვდომა სენსიტიურ ინფორმაციაზე, რაც თავდასხმის დამატებითი მიზეზი ხდება.

კიბერშეტევის ტიპების მარტივი განმარტებები:

არამიზნობრივი შეტევა

- კიბერსაფრთხის ყველაზე გავრცელებული და მზაკვრული ფორმა;
- არ არის მიმართული კონკრეტულ ინდივიდზე ან ორგანიზაციაზე;
- კიბერ დამნაშავეების მიზანია რაც შეიძლება მეტი კომპიუტერის, ინდივიდის და ორგანიზაციის მოცვა;
- მავნე პროგრამული უზრუნველყოფა, კომპიუტერული ჭიები და ვირუსები ყოველგვარი შერჩევის გარეშე იგზავნება ელ.ფოსტის უამრავ მისამართზე;
- არამიზნობრივი კიბერ შეტევა მიზნობრივზე ადვილი აღსაკვეთი და ნაკლები ზიანის მომტანია.

მიზნობრივი შეტევა

- მიმართულია კონკრეტულ პირებზე ან ორგანიზაციებზე;
- კიბერ დამნაშავეები ინტერესის ობიექტის შერჩევით, კონკრეტული მიზნით მოქმედებენ;
- მსგავსი შეტევების განხორციელებას თვეები სჭირდება და შეიძლება მოიცავდეს სოციალურ ინჟინერიას, ფიშინგს, სპეციალურად შექმნილ მავნე პროგრამებს, უწყვეტ შეტევას და ბოტნეტებს;
- შეტევის სამიზნეები გასცდა სახელმწიფო ორგანოებსა და სამხედრო ბაზებს და მოიცვა ორგანიზაციები, მედია, საკომუნიკაციო და კრიტიკული ინფრასტრუქტურა.

კიბერშეტევის ტიპების გაგება ციფრულ სამყაროში ეფექტურ ნავიგაციას გაგიმარტივებთ.

ალბათ, ფიქრობთ, „რატომ ინტერესდებიან კიბერკრიმინალები ჩემზე შეტევის განხორციელებით?“ ეს მართებული კითხვაა, განსაკუთრებით მათთვის, ვინც ჰუმანიტარულ საქმიანობას, აქტივიზმს თუ ქალთა უფლებების დაცვას ემსახურება. ერთი შეხედვით, კიბერშეტევების მიღმა მოტივაცია შეიძლება დამაბნეველი ჩანდეს, მაგრამ მისი გააზრება კრიტიკულად მნიშვნელოვანია.

მოტივების გამოაშკარავება: რატომ გირჩევენ სამიზნედ?

1. ზემოქმედება და დესტრუქცია

თქვენი არსებითი როლი: თქვენი, როგორც აქტივისტის, მშვიდობის მშენებლის ან საზოგადოების ლიდერის მისიაა საზოგადოებრივი აზრის ფორმირება და პოლიტიკის შემუშავებაზე ზემოქმედების მოხდენა.

კიბერ საფრთხე: შესაძლოა, კიბერ დამნაშავეებმა თქვენზე შეაჩერონ არჩევანი, რათა ხელი შეგიშალონ მნიშვნელოვან საქმიანობაში. მიზანში თქვენი ამოღებით, ქაოსის შექმნისა და პოზიტიური ინიციატივების გავრცელების შეფერხებისკენ მიისწრაფვიან.

2. სენსიტიურ ინფორმაციაზე წვდომის მიღება

კრიტიკულ მონაცემებზე წვდომა: თქვენი ყოველდღიური საქმიანობიდან გამომდინარე, სოციალურ საკითხებთან დაკავშირებულ არაერთ სენსიტიურ ინფორმაციასთან გაქვთ წვდომა.

კიბერ საფრთხე: შეიძლება, კიბერ დამნაშავეები ცდილობდნენ ამ ინფორმაციის მოპარვას ან მანიპულირებას სარგებლის მიღების მიზნით. იქნება ეს პირადი მიზნებისთვის გამოყენება თუ საზოგადოებრივი აზრის შეცვლის მცდელობა, თქვენ ხელთ არსებული ღირებული ინფორმაცია კიბერ დამნაშავეების სამიზნე ხდება.

ამ მოტივების ცოდნა კიბერ მედეგობისკენ გადადგმული პირველი ნაბიჯია.

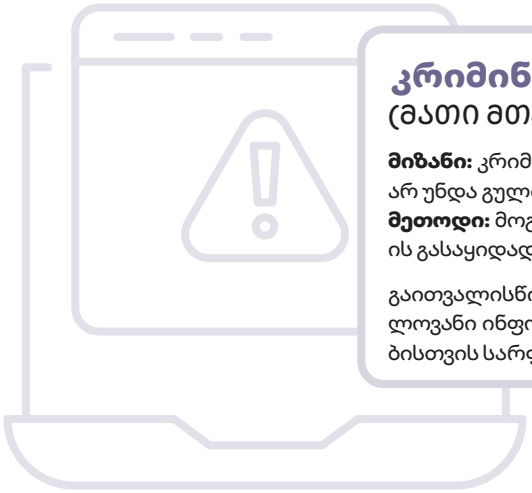
> ჩვენი, როგორც კიბერ უსაფრთხოების ექსპერტების როლია, დაგიცვათ, რომ არ გახდეთ არამიზნობრივი კიბერშეტევის შემთხვევითი მსხვერპლი. იმ შემთხვევაში, თუ ჰაკერი კონკრეტულად თქვენ გირჩევთ სამიზნედ, დიდი ალბათობით, ის იპოვის გზას და ალმოაჩენს თქვენს სისუსტეს. ამ შემთხვევაში, ჩვენი როლია კიბერშეტევის რაც შეიძლება დიდი ხნით გადავადება
>
> ვლად მაზურაკი,
> კიბერუსაფრთხოების ექსპერტი.

მოკლედ, კიბერდამნაშავეების ტიპების შესახებ:

„ჰაკტივისტები“
(დიახ, ჰაკერი აქტივისტები ნამდვილად არსებობენ)

მოტივი: ამოძრავებთ პოლიტიკური ან სოციალური საკითხები.
მისია: საკუთარი მიზნის ადვოკატირება ან სუბიექტურად აღქმული უსამართლობის გაპროტესტება
საყვარელი კიბერ თავდასხმა: ვებსაიტების იერსახის ცვლილება (Defacement), სენსიტიური ინფორმაციის გამჟღავნება ან ონლაინ აქტივობების შეფერხება.

„ჰაკტივისტების“ საქმიანობის ბუნებიდან გამომდინარე, ადვილი შესაძლებელია, გახდეთ მათი თავდასხმის სამიზნე. მნიშვნელოვანია, იყოთ ინფორმირებულნი და გამოიჩინოთ სიფრთხილე.



კრიმინალური ორგანიზაციები
(მათი მთავარი მოტივაცია ფულია)

მიზანი: კრიმინალური საქმიანობის გაფართოება, რასაც არ უნდა გულისხმობდეს ეს.
მეთოდი: მოგების მიღების მიზნით, პირადი ინფორმაციის გასაყიდად მოპარვა.

გაითვალისწინეთ, რომ თქვენ ხელთ არსებული მნიშვნელოვანი ინფორმაცია, შესაძლოა, მსგავსი ორგანიზაციებისთვის სარფიან სამიზნედ გადაიქცეს.

სახელმწიფოს მიერ დაფინანსებული აქტორები
(საგარეო თუ საშინაო)

ჩართულობა: წარმოადგენენ მთავრობის ან სახელმწიფოს მიერ დაფინანსებულ ერთეულებს.
მიზანი: განსხვავებული აზრის დათრგუნვა და ოპოზიციის აქტივობის კონტროლი.
რისკის ხარისხი: მათ ხელთ არსებული ტექნიკურად განვითარებული შესაძლებლობები დიდ რისკს უქმნის ინდივიდებსა და ორგანიზაციებს.

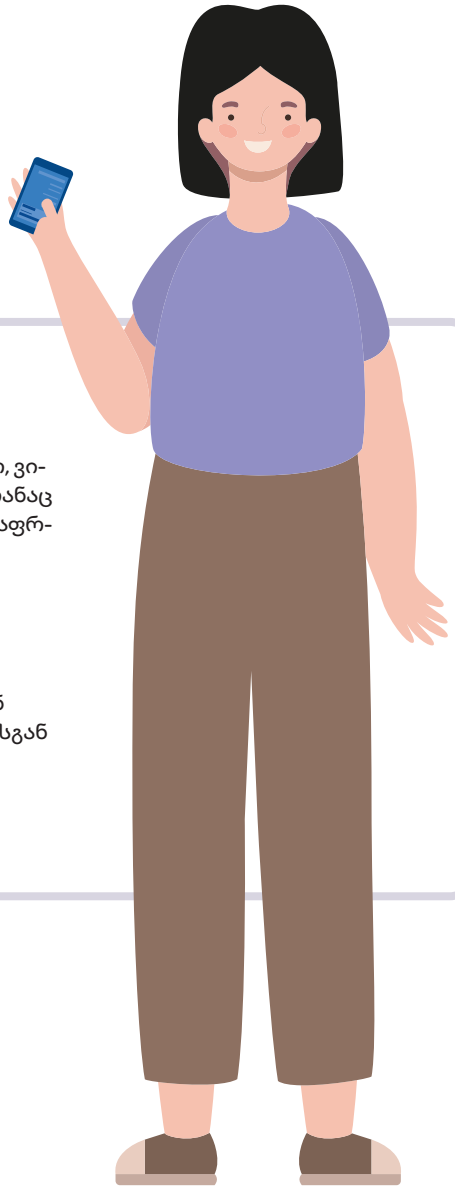
აქტივისტების, მშვიდობის მშენებლებისა და საზოგადოების ლიდერებისაკენ მიმართული კიბერსაფრთხეების მოტივების გაგებას გადამწყვეტი მნიშვნელობა აქვს. ეს პოტენციური რისკების გააზრებასა და პროაქტიული ნაბიჯების გადადგმაში დაგეხმარებათ კიბერუსაფრთხოების მისაღწევად საიმედო გზების შესამუშავებლად.

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

1. **უნივერსალური მოწყვლადობა:** კიბერშეტევის მსხვერპლი შეიძლება გახდეს ნებისმიერი, მისგან დაცული არავინაა. თქვენმა პროფესიულმა საქმიანობამ, შესაძლებელია, ეს რისკი უფრო მეტად გაზარდოს.
2. **მიზნობრივი vs არამიზნობრივი შეტევა:** მათ შორის მთავარი განსხვავება არის განზრახვა. მიზნობრივი შეტევა კონკრეტული ინდივიდებისკენ არის მიმართული, მაშინ როცა, არამიზნობრივი უფრო ფართო ქსელზე ვრცელდება.
3. **კიბერდამნაშავეების განსხვავებული მოტივები:** არსებობენ სხვადასხვა ტიპის კიბერდამნაშავეები და თითოეულ მათგანს განსხვავებული მიზანი და მოტივაცია ამოძრავებს.
4. **გლობალური დაცვა:** კიბერუსაფრთხოებისთვის პრიორიტეტის მინიჭება მხოლოდ თქვენ არ გიცავთ, ის ვრცელდება თქვენს კოლეგებზე, ბენეფიციარებსა და ორგანიზაციაზეც.

გახსოვდეთ, ამ საკვანძო საკითხების გააზრება არა მხოლოდ აძლიერებს თქვენს ინდივიდუალურ თავდაცვას, არამედ უზრუნველყოფს თქვენი პროფესიული ეკოსისტემის კოლექტიურ მედეგობას.

> მას, ვინც იცნობს თავის თავს და მტერს, ასეულობით ბრძოლაშიც კი არ ემუქრება საფრთხე
>
> სუნ ძი



შეამოწმეთ თქვენი ცოდნა

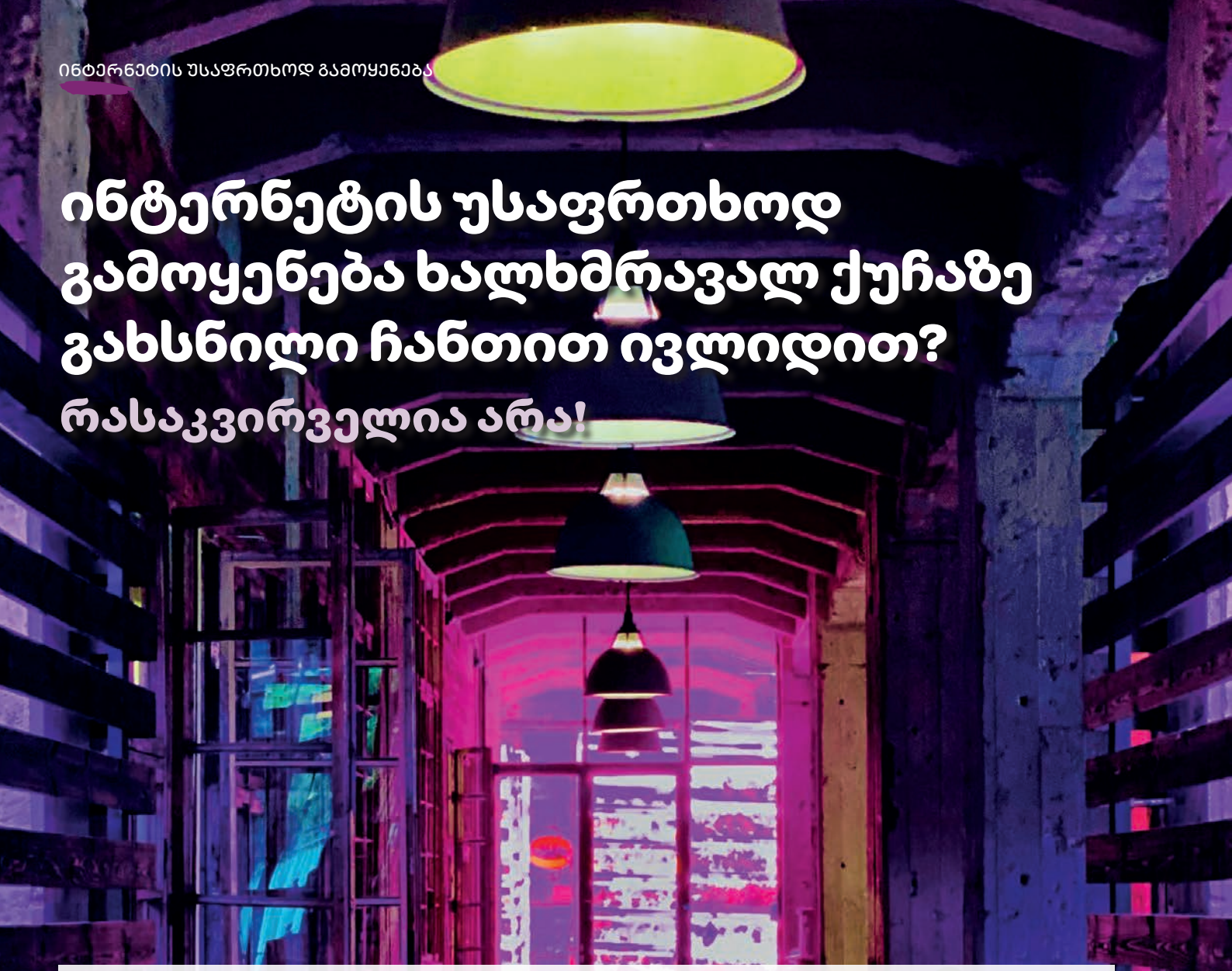
ცნობილმა აქტივისტმა, ნინომ ფიშინგის ელექტრონული წერილი მიიღო, ვითომ იმ ადამიანების უფლებების დამცველი ორგანიზაციისგან, რომელთანაც თანამშრომლობს. აღნიშნული ელ. ფოსტა მას ბმულზე გადასვლას და უსაფრთხოების ხარვეზის გამო, პირადი მონაცემების განახლებას მოუწოდებდა.

რომელი ტიპის კიბერ თავდასხმის მსხვერპლი გახდა ნინო?

1. მიზნობრივი შეტევა მისი ინფორმაციის მოსაპარად
2. არამიზნობრივი შეტევა მისი ინფორმაციის მოსაპარად
3. მიზნობრივი შეტევა დანაშაულებრივი/კრიმინალური ორგანიზაციისგან
4. არამიზნობრივი შეტევა დანაშაულებრივი/კრიმინალური ორგანიზაციისგან

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები

ინტერნეტის უსაფრთხოდ გამოყენება ხალხმრავალ ქუჩაზე გახსნილი ჩანთით ივლიდით? რასაკვირველია არა!



წარმოიდგინეთ, რომ თბილისის ერთ-ერთი ხალხმრავალი ქუჩის გავლით, სამსახურში მიემართებით. იმის უზრუნველყოფა, რომ თქვენი ჩანთა საიმედოდ არის დახურული, ქუჩის გადაკვეთამდე ორივე მხარეს გახედვა და გარემოსთან ადაპტირება, თქვენთვის მეორე ბუნება გახდება. ერთი შეხედვით დაცულ სივრცეებშიც კი, რისკების შესამცირებლად გაცნობიერებულობა, სიფრთხილე და პროაქტიული ზომების მიღება თქვენ ცნობიერში ღრმად გამჯდარ ჩვევად იქცევა.

მსგავსი პრინციპები მოქმედებს ონლაინ სამყაროში ნავიგაციის დროს. ინტერნეტის უსაფრთხოდ გამოყენება ქუჩებში უსაფრთხო სეირნობის პრინციპებს ირეკლავს და ხაზს უსვამს გაცნობიერებულობას, სიფრთხილესა და პროაქტიული ზომების მიღებას რისკის შესამცირებლად.

ისწავლეთ, როგორ გამოიჩინოთ წინდახედულობა ციფრულ სამყაროში. თაღლითობისა და მონაცემების მოპარვის მიზნით, კიბერკრიმინალები სულ უფრო დახვეწილ მეთოდებს იყენებენ. თავდაპირველად, შეიძლება რთულ გამოწვევად მოგეჩვენოთ, მაგრამ კიბერუსაფრთხოების ზომების გამოყენება იმ ჩვევების მსგავსია, რომლებსაც ქუჩებში ნავიგაციის ან სახლიდან გასვლის დროს იყენებთ – პრაქტიკასთან ერთად, ეს ჩვევები თქვენი ცხოვრების განუყოფელი ნაწილი გახდება.

ასპექტი	ქუჩებში უსაფრთხოდ სეირნობა	ინტერნეტის უსაფრთხოდ გამოყენება
სიფრთხილისა და გაცნობიერებულობის გამოჩენა	იყავით ყურადღებიანი თქვენი გარემოცვის მიმართ. მოერიდეთ ცუდად განათებულ ადგილებს და გამოიჩინეთ სიფრთხილე უცნობ პირებთან.	გამოიჩინეთ სიფრთხილე ფიშინგის მახეებთან და თაღლითურ ვებსაიტებთან ინტერაქციის დროს.
უსაფრთხოების დადასტურება	აირჩიეთ უსაფრთხო მარშრუტები და გადაამოწმეთ უბნის სანდოობა ფიზიკური უსაფრთხოების მხრივ.	გადაამოწმეთ ვებსაიტების ავთენტურობა პერსონალური ინფორმაციის გაზიარებამდე.
პრევენციული ზომების მიღება	მიიღეთ პრევენციული ზომები, როგორიცაა კარების ჩაკეტვა, ჩანთის დახურვა და ძვირფასეულობის დაცვის უზრუნველყოფა.	გამოიყენეთ უსაფრთხოების ინსტრუმენტები, განაახლეთ ბრაუზერები და შეარჩიეთ ინფორმაციის დაცვის (კონფიდენციალურობის) მკაცრი პარამეტრები.
წესებისა და მითითებების დაცვა	დაემორჩილეთ საგზაო მოძრაობის წესებს და მიჰყევით საგზაო ნიშნებს და მითითებებს.	მიჰყევით კიბერუსაფრთხოების საუკეთესო პრაქტიკებს და დაიცავით ვირტუალურ (ონლაინ) სივრცეში ყოფნის წესები.
უსაფრთხოების პერიოდული შემოწმება	ჩაატარეთ საკეტების, კარებისა და შემოგარენის პერიოდული შემოწმება თქვენი ფიზიკური უსაფრთხოების უზრუნველყოფის მიზნით.	რეგულარულად განაახლეთ ოპერაციული სისტემები, ბრაუზერები და უსაფრთხოების პროგრამული უზრუნველყოფა.

MIKE SWIGUNSKI | UNSPLASH

სწრაფი გზამკვლევი თაღლითური ვებსაიტების გამოსავლენად

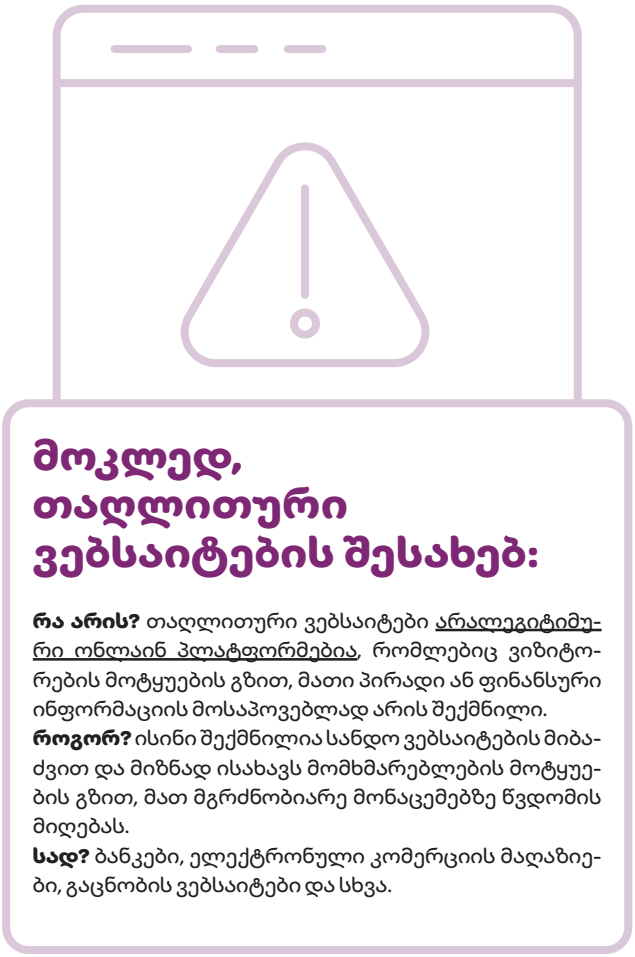
1 **შეამოწმეთ ვებსაიტის მისამართი (URL):** გულდასმით დაათვალიერეთ ვებსაიტის მისამართი (URL) არასწორი მართლწერის, ზედმეტი სიმბოლოების ან უჩვეულო დომენების აღმოსაჩენად.
- **ლეგიტიმური:** https://www.example.com
- **ფიშინგი:** https://www.exaample.com (არასწორი მართლწერა), https://www.example.pf (უჩვეულო დომენი)

2 **ყურადღება გაამახვილეთ HTTPS-ზე:** დარწმუნდით, რომ ვებსაიტი იყენებს HTTPS-ს HTTP-ის ნაცვლად. S მიუთითებს მონაცემების დაცული არხით გადაცემაზე.
- **ლეგიტიმური:** https://www.securewebsite.com
- **ფიშინგი:** http://www.insecurewebsite.com (დაცული არხით გადაცემისთვის აკლია S)

3 **ყურადღება მიაქციეთ ვებსაიტის დიზაინს:** ფრთხილად იყავით არაპროფესიონალურად შემუშავებულ ან ისეთ ვებსაიტებთან, რომლებსაც აქვთ მრავალი ამომხტომი ფანჯარა (Pop-ups).
- **ლეგიტიმური:** პროფესიონალური აგებულება და თანმიმდევრული ბრენდინგი.
- **ფიშინგი:** დაბალხარისხიანი დიზაინი, შეუთავსებელი ლოგოები და მრავალი ამომხტომი ფანჯარა (Pop-ups).

4 **გადაამოწმეთ საკონტაქტო ინფორმაცია:** ლეგიტიმური ვებსაიტები მკაფიოდ უთითებენ საკონტაქტო ინფორმაციას. არ ენდოთ ვებსაიტს, თუ არცერთი მოწოდებული საკონტაქტო ინფორმაცია არ არის ხელმისაწვდომი ან თუ დეტალები საეჭვოდ გამოიყურება.
- **ლეგიტიმური:** საკონტაქტო ინფორმაციის გვერდი არის დეტალური და მითითებულია სწორი მისამართი, ტელეფონის ნომერი და ელ. ფოსტა.
- **ფიშინგი:** საკონტაქტო ინფორმაცია არ არის მითითებული, ან საეჭვოდ გამოიყურება. მაგალითად, მოცემულია ზოგადი ხასიათის ელ. ფოსტის მისამართი.

5 **გადაატარეთ მაუსი ბმულებზე:** გადაატარეთ მაუსი ბმულებზე დანიშნულების URL-ის შესამოწმებლად. მოერიდეთ ელ. ფოსტით მიღებულ ბმულებზე გადასვლას (დაწკაპუნებას); სანაცვლოდ, თავად აკრიფეთ URL-ი ვებ ბრაუზერში.
- **ლეგიტიმური:** გადახედეთ ბმულს მასზე მაუსის გადატარებით. გამოსახული ინფორმაცია უნდა ემთხვეოდეს მითითებულ ტექსტს.
- **ფიშინგი:** ბმულზე მაუსის გადატარებით გამოავლინეთ დანიშნულების URL-ი, რომელიც უნდა ემთხვეოდეს ბმულზე მითითებულ ტექსტს. მაგალითად, http://www.trustworthy.com (ბმულზე მითითებული ტექსტი), მაგრამ დანიშნულების ბმულით გადავდივართ http://www.phishingsite.com-ზე.



მოკლედ, თაღლითური ვებსაიტების შესახებ:

რა არის? თაღლითური ვებსაიტები არალეგიტიმური ონლაინ პლატფორმებია, რომლებიც ვიზიტორების მოტყუების გზით, მათი პირადი ან ფინანსური ინფორმაციის მოსაპოვებლად არის შექმნილი.
როგორ? ისინი შექმნილია სანდო ვებსაიტების მიბაძვით და მიზნად ისახავს მომხმარებლების მოტყუების გზით, მათ მგრძნობიარე მონაცემებზე წვდომის მიღებას.
სად? ბანკები, ელექტრონული კომერციის მაღაზიები, გაცნობის ვებსაიტები და სხვა.

სწრაფი გზამკვლევი ფიშინგ თაღლითობის აღმოსაჩენად:

1 **რეგულარულად შეამოწმეთ თქვენი ანგარიშები:** ფიშინგის მიზნით გამოგზავნილ ელ. ფოსტაში, შესაძლოა, თქვენს ანგარიშზე მომხდარი საეჭვო აქტივობების შესახებ გაცნობონ და პრობლემის მოსაგვარებლად, თანდართულ ბმულზე გადასვლა მოგიწოდონ.
მაგალითი: „სასწრაფოდ: თქვენი ანგარიში გატეხილია. ინფორმაციის გადასამოწმებლად გადადით ბმულზე“.

2 **ელ. წერილი, რომელიც თქვენგან მოითხოვს გადაუდებელ ქმედებას:** ფიშერები ხელოვნურად ქმნიან სასწრაფოების შეგრძნებას.
მაგალითი: „თქვენი ანგარიშის აქტიური სტატუსი შეჩერდება, თუ არ დაადასტურებთ დეტალებს მომდევნო 24 საათის განმავლობაში. დაუყოვნებლივ გადადით ვებ-ბმულზე, რათა თავიდან აიცილოთ შეფერხება“.
მაგალითი: „შეთავაზების ვადა იწურება! ჯილდოს მისაღებად, იმოქმედე ახლავე!“

3 **ელ. წერილები გრამატიკული შეცდომებით და არაპროფესიონალური მართლწერით:** ლეგიტიმური ორგანიზაციები კომუნიკაციის პროფესიონალურ სტილს ინარჩუნებენ.
მაგალითი: „ძვირფასი იუზერო, თქვენი ანგრიში გატეხილია. უსაფრთხების გამო განაახლეთ პაროლი“.
მაგალითი: „ექსკლუზიური პრიზის მისაღებად, მიჰყევით მოცემულ ბმულს“ ნაცვლად, „დააწკაპუნეთ აქ თქვენი ექსკლუზიური პრiზისთვის“.

4 **საჯარო ელ.ფოსტის დომენის გამოყენება:** ხშირად, ფიშინგ თაღლითები საჯარო ელ. ფოსტის დომენებს იყენებენ.
მაგალითი: “service@legitimatecompany.com”-ის ნაცვლად, “service@gmail.com”.

5 **შეამოწმეთ ელექტრონული ფოსტის მისამართი:** კიბერკრიმინალები ლეგიტიმურ ელ. ფოსტის მისამართებს ჰბაძავენ.
მაგალითი: “support@paypalcom.” -ის ნაცვლად “support@paypa1.com”.

6 **ელ. ფოსტის სათაურის ველში ზოგადი ტექსტი:** ფიშინგ ელ. წერილები ხშირად იყენებენ ბუნდოვან სათაურებს.
მაგალითი: „მნიშვნელოვანი ინფორმაცია“ შეტყობინების არსის მითითების გარეშე.

მოკლედ, ფიშინგის კიბერთაღლითობის შესახებ

რა არის? ფიშინგი კიბერთაღლითობის ფორმაა, რომლის მიზანია პირების მოტყუების გზით, ისეთი სენსიტიური ინფორმაციის მოპარვა, როგორიცაა მომხმარებლის სახელები, პაროლები, ფინანსური ინფორმაცია და შემდგომში, მოპარული ინფორმაციის მავნე მიზნებისთვის გამოყენება.
როგორ? შეტევის დროს გამოიყენება ელ. ფოსტა, მოკლე ტექსტური შეტყობინება ან კომუნიკაციის სხვა ფორმა, რომელიც წარმოჩენილია როგორც სანდო წყაროსგან მიღებული გზავნილი.
სად? ელ. ფოსტა, სოციალური მედია, WhatsApp-ის ჩატი და სხვა.

გლობალურად, ფიშინგ ელ. წერილების ყველაზე გავრცელებული სათაურები:

Google: თქვენ სახელი ნახსენებია დოკუმენტში „სტრატეგიული გეგმის მონახაზი“
HR: მნიშვნელოვანია: ცვლილებები ჩაცმის სტილის რეგულაციაში
HR: შვებულების პოლიტიკის განახლება
Adobe sign: სამუშაოს შესრულების შეფასება, დაუყოვნებლივ შეამოწმეთ პაროლი
დაადასტურეთ თქვენი შეფასება
ძირითადი პუნქტები დღევანდელი შეხვედრიდან
USAA: ანგარიშის შეჩერება
თანამშრომლის ხარჯების კომპენსაცია [[email]]

წყარო 16: ყველაზე გავრცელებული ფიშინგ ელ. ფოსტის თემები 2022 წლის მესამე კვარტლისთვის (KnowBe4)

ფიშინგი უფრო და უფრო პოპულარული ხდება კიბერკრიმინალებს შორის:

გლობალურად, ყველა გაგზავნილი ელ. ფოსტის დაახლოებით **1,2%** ფიშინგის მცდელობას წარმოადგენს. მსოფლიოს მასშტაბით ორგანიზაციების **81%** აღნიშნავს ელექტრონული ფოსტის ფიშინგ კიბერშეტევების ზრდას. 2022 წელს, Verizon-ის „მონაცემების გამჟღავნების ანგარიშის“ თანახმად, ფიშინგ თაღლითობა მონაცემების გამჟღავნების **36%**-ზეა პასუხისმგებელი.

თაღლითური ვებსაიტები და ფიშინგ თაღლითობა: მსგავსი, მაგრამ განსხვავებული

თაღლითური ვებსაიტები არალეგალურ ონლაინ პლატფორმებს წარმოადგენს. მათი მიზანია ვიზიტორების მოტყუების გზით, მათი პირადი ან ფინანსური ინფორმაციის მოპარვა. ხშირად, თაღლითური ვებსაიტები ლეგიტიმურ, სანდო წყაროებს ჰბაძავენ.

მეორეს მხრივ, ფიშინგ თაღლითობა ისეთი მოტყუებითი მეთოდების გამოყენებას გულისხმობს, როგორიცაა შეცდომაში შემყვანი ელ. წერილი ან სხვა ტიპის კომუნიკაცია, როდესაც თავდამსხმელი რეპუტაციის მქონე სანდო წყაროდ წარმოაჩენს საკუთარ თავს და პირების მოტყუების გზით, ცდილობს მათი სენსიტიური ინფორმაციის მოპოვებას.

ინტერნეტის უსაფრთხოდ გამოყენება, ხალხმრავალ ქუჩებში უსაფრთხოდ სეირნობის მსგავსია. სიფრთხილის, გაცნობიერებულობის და რისკების წინააღმდეგ პროაქტიული ზომების ის პრინციპები, რომლებიც ღრმად გვაქვს ჩანერგილი ყოველდღიურ ჩვენებში ჩვენი ფიზიკური უსაფრთხოების უზრუნველყოფის მიზნით, რეზონანსულია ციფრულ სამყაროში.

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

1. პრაქტიკასთან ერთად, ფიზიკური ჩვევების მსგავსად, ვირტუალური ჩვევები თქვენი მეორე ბუნება გახდება.
2. გამოიჩინეთ სიფრთხილე ფიშინგ თაღლითობასთან და თაღლითურ ვებსაიტებთან.
3. პირადი ინფორმაციის გაზიარებამდე, გადაამოწმეთ ვებსაიტის ავთენტურობა.
4. მიიღეთ უსაფრთხოების ზომები, განაახლეთ ბრაუზერები და გამოიყენეთ კონფიდენციალურობის მკაცრი პარამეტრები.
5. რეგულარულად განაახლეთ ოპერაციული სისტემები, ბრაუზერები და უსაფრთხოების პროგრამული უზრუნველყოფა.

ახლა, ონლაინ სამყარო უფრო უსაფრთხო გახდა როგორც თქვენთვის, ისე თქვენ გარშემო მყოფი ადამიანებისთვის.

შეამოწმეთ თქვენი ცოდნა:

ელ. ფოსტის ქვემოთ ჩამოთვლილი სათაურებიდან რომელი ასოცირდება ყველაზე გავრცელებულ ფიშინგ წერილებთან?
(აირჩიეთ ყველა, რომელიც შეესაბამება):

1. თქვენი ანგარიში გატეხილია. შეამოწმეთ ახლავე!
2. სასწრაფოდ: გადაუდებელი ქმედებაა საჭირო სახელფასო განახლებისთვის
3. სიახლეების გამოწერის დადასტურება
4. უფასო საჩუქარი! მიჰყევით ბმულს თქვენი პრიზის მისაღებად
5. მნიშვნელოვანია: გადახედეთ და დაადასტურეთ დოკუმენტი
6. უსაფრთხოების გაფრთხილება: თქვენს ანგარიშზე გამოვლინდა უჩვეულო ავტორიზაციის აქტივობა
7. გილოცავ! თქვენ ლატარია მოიგეთ.

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები

საჯარო Wi-Fi: კიბერ კრიმინალების თავშესაფარი

პროფესიონალური რჩევა:

თუ არ გეგმავთ სახურავებიდან ყვირილს, მაშინ საჯარო Wi-Fi ქსელში ინფორმაციას ნუ გაამხელთ.

სალომე, საუკეთესო მეგობარ ნინოსთან ერთად, მათ საყვარელ რესტორანში სასიამოვნო სადილს მიირთმევს. მეგობრები ცოცხალი საუბრით ტკბებიან, ერთმანეთს პირად ამბებს და ზაფხულის თავგადასავლებს უზიარებენ. დიალოგი სამუშაოს განხილვაზე გადადის, რადგან ისინი ერთობლივ პროექტზე თანამშრომლობას გეგმავენ.

საუბრის განმავლობაში, სალომე და ნინო ერთმანეთს კონფიდენციალურ ინფორმაციას უზიარებენ იმ თავშესაფრების ადგილმდებარეობის შესახებ, რომლებიც გენდერული ნიშნით ძალადობის მსხვერპლი ქალებისთვის დააარსეს. განიხილავენ, თუ როგორ დაეხმარონ თავშესაფრის მობინადრეებს და მომდევნო დღეს სტუმრობას გეგმავენ.

ახლა, წარმოიდგინეთ სცენარი, სადაც ამ საუბრის შინაარსი საჯარო ხდება და რესტორანში მყოფი ყველა პირი მათ უსმენს.

შესაძლოა, ეს შედარება გაზვიადებულად მოგეჩვენოთ, მაგრამ ის ზუსტად ასახავს საჯარო Wi-Fi ქსელების დაუცველობას, რომლის თითოეული მომხმარებელი შეუზღუდავ წვდომას იღებს საჯარო უსადენო ლოკალური ქსელით გადაცემულ ინფორმაციაზე.

Wi-Fi Hotspot-თან დაკავშირების შემთხვევაში, Hotspot-ის მფლობელს თქვენი ონლაინ აქტივობების და ზოგიერთ შემთხვევაში, ფიზიკური მოძრაობების გაკონტროლების უფლებას ანიჭებთ.

გაითვალისწინეთ ის შესაძლო შედეგები, რომლებიც კაფეში მუშაობას მოსდევს. სენსიტიური ინფორმაციის დასამუშავებლად სამუშაო კომპიუტერის გამოყენება, ელ. ფოსტით მიმოწერა ან კონფიდენციალური დეტალების გაზიარება - ყველა ეს მონაცემი ხილული და ხელმისაწვდომი ხდება საჯარო Wi-Fi ქსელის გამოყენების დროს და ჰაკერებისთვის პოტენციურ სათამაშო მოედნად გადაიქცევა.

MARK BILLANTE | UNSPLASH

თუ გესაჭიროებათ გარკვეული სენსიტიური ინფორმაციის ნახვა ან პაროლით დაცულ ანგარიშებზე წვდომა, ამისათვის არსებობს რამდენიმე უსაფრთხო მეთოდი:

1. გამოიყენეთ Hotspot (პორტატული ინტერნეტ კავშირი)

სენსიტიურ ინფორმაციაზე ან პაროლით დაცულ ანგარიშებზე წვდომის დროს, პირადი ინტერნეტ კავშირის (Hotspot) გამოყენებამ, შესაძლოა, გააძლიეროს თქვენი უსაფრთხოება. ცხელი წერტილის (Hotspot) გამოსაყენებლად, მიჰყევით ქვემოთ მოცემულ ნაბიჯებს:

ა. გააააქტიურეთ ცხელი წერტილი (Hotspot):

- თქვენს სმარტფონზე გადადით პარამეტრებზე
- მოძებნეთ Hotspot ან Tethering
- ჩართეთ Hotspot და დააყენეთ ძლიერი პაროლი.

ბ. დააკავშირეთ მოწყობილობები:

- დაუკავშირეთ თქვენი კომპიუტერი ან სხვა მოწყობილობები Hotspot-ს.
- დამატებითი უსაფრთხოებისთვის, დარწმუნდით, რომ თქვენი Hotspot დაცულია პაროლით.

გ. იხილეთ სენსიტიური მონაცემები:

- Hotspot-თან დაკავშირების შემდეგ, უსაფრთხოდ ნახეთ მგრძნობიარე ინფორმაცია ან შედით პაროლით დაცულ ანგარიშებზე.

შენიშვნა: ზემოხსენებული წარმოადგენს ზოგად სახელმძღვანელო მითითებებს და შეიძლება განსხვავდებოდეს თქვენი მოწყობილობისა და ოპერაციული სისტემის მიხედვით.

2. გამოიყენეთ VPN (ვირტუალური კერძო ქსელი)

VPN-ის გამოყენება ეფექტური გზაა თქვენი ონლაინ აქტივობების უსაფრთხოების უზრუნველსაყოფად, განსაკუთრებით, საჯარო Wi-Fi ქსელით სარგებლობის დროს. ქვემოთ მოცემულია VPN-ის გამოყენების სწრაფი გზამკვლევი Windows-ისა და Mac-ისთვის:

ა. შეარჩიეთ VPN-ის პროვაიდერი:

- შეარჩიეთ სანდო რეპუტაციის მქონე VPN სერვისი და შექმენით პირადი ანგარიში.

ბ. ჩამოტვირთეთ და დააყენეთ პროგრამა:

- ჩამოტვირთეთ VPN კლიენტი თქვენი ოპერაციული სისტემისთვის.
- დააყენეთ პროგრამული უზრუნველყოფა პროვაიდერის მიერ მოწოდებული ინსტრუქციის შესაბამისად.

გ. დაუკავშირდით სერვერს:

- გაუშვით VPN-ის პროგრამა.
- აირჩიეთ სერვერის მდებარეობა და დაამყარეთ უსაფრთხო კავშირი.

დ. იხილეთ სენსიტიური ინფორმაცია:

- საჯარო ქსელებით სარგებლობის დროს, აქტიური VPN-ის გამოყენებით სენსიტიურ ინფორმაციაზე უსაფრთხო წვდომის მიღებას შეძლებთ.

შენიშვნა: ზემოხსენებული წარმოადგენს ზოგად სახელმძღვანელო მითითებებს და შეიძლება განსხვავდებოდეს თქვენი მოწყობილობისა და ოპერაციული სისტემის მიხედვით.

3. დაელოდეთ, სანამ შეძლებთ სანდო და არასაჯარო Wi-Fi ქსელის გამოყენებას

როდესაც საქმე ეხება უაღრესად მგრძნობიარე მონაცემებთან მუშაობას, სანდო და არასაჯარო Wi-Fi ქსელზე წვდომის მიღებამდე დაცდა ყველაზე უსაფრთხო არჩევანია. საჯარო ქსელების გამოყენებისგან თავიდან არიდება, გამორიცხავს მათთან დაკავშირებული რისკების წარმოშობას.

გახსოვდეთ, მონაცემების უსაფრთხოების დაცვა პირველხარისხოვანია, ხოლო მათზე წვდომისთვის სწორი მეთოდის არჩევა, მონაცემების სენსიტიურობისა და გადაუდებლობის ხარისხზეა დამოკიდებული.

ყურადღების ცენტრში:

მიუხედავად იმისა, რომ მოსახერხებელია, საჯარო Wi-Fi მრავალი რისკის შემცველია

კიბერკრიმინალებს თქვენს მოწყობილობასა და Wi-Fi როუტერს შორის გადაცემულ მონაცემებზე წვდომის მიღება და პოტენციურად სენსიტიური ინფორმაციის ხელში ჩაგდება შეუძლიათ.

დაშიფვრის ნაკლებობა საჯარო Wi-Fi-ით გადაცემული მონაცემების დაუცველობაზე მიანიშნებს.

მომხმარებლების მოტყუების და მათი მავნე ქსელებთან დაკავშირების მიზნით, **კიბერ თავდამსხმელებმა** ცრუ სახელებით შეიძლება შექმნან WiFi Hotspot-ები.

.

ჰაკერებმა შეიძლება გამოიყენონ პაკეტების სნიფერები (Packet Snipping) რაც, სენსიტიურ ინფორმაციაზე წვდომის მიღების მიზნით, ქსელში გაგზავნილი ინფორმაციის პაკეტების აღკვეთას და გაშიფვრას გულისხმობს.

რა არის VPN (ვირტუალური კერძო ქსელი)?

VPN-ი, ან ვირტუალური კერძო ქსელი, თქვენი უჩინმაჩინის ქუდია ციფრულ სამყაროში. VPN-ის გამოყენების დროს, თქვენი მონაცემები დაშიფრულ ნიღაბს ატარებენ სპეციალურ მისიაზე მყოფი საიდუმლო აგენტის მსგავსად.

ყურადღების ცენტრში:

VPN-ის პროვაიდერის შერჩევა, რა უნდა გავითვალისწინოთ:

უსაფრთხოების და კონფიდენციალურობის მახასიათებლები: დარწმუნდით, რომ VPN-ი თქვენი მონაცემების დასაცავად უზრუნველყოფს ძლიერ დაშიფვრას, No-Logs პოლიტიკას (გულისხმობს, რომ VPN-ის პროვაიდერი არ აკონტროლებს, არ ინახავს ან არ აზიარებს ქსელში გადაცემულ ინფორმაციას) და უსაფრთხოების გაფართოებულ პროტოკოლებს.

სერვერის ქსელი და მდებარეობები: სერვერის მრავალფეროვანი და ფართოდ განშტოებული ქსელი აუმჯობესებს ვირტუალურ სამყაროში თქვენს გამოცდილებას. შეარჩიეთ VPN-ი ისეთი სერვერებით, რომლებიც სტრატეგიულად არის განთავსებული მთელი მსოფლიოს მასშტაბით.

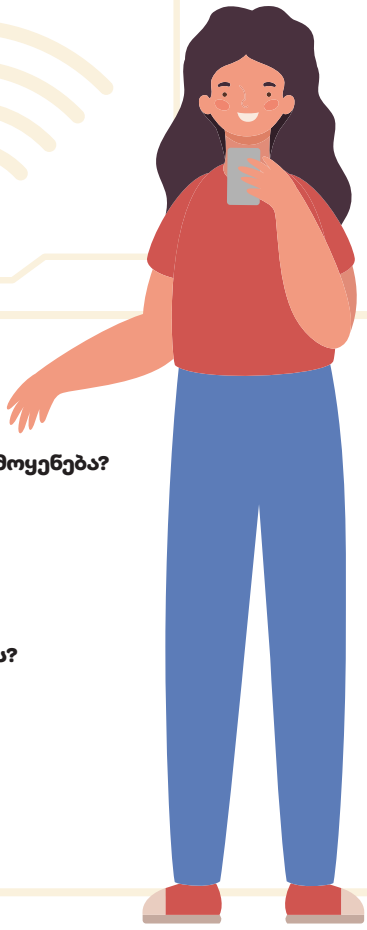
კავშირის სიჩქარე: აირჩიეთ VPN-ი, რომელიც კავშირის სწრაფ და საიმედო სიჩქარეს უზრუნველყოფს, რაც არსებითია უწყვეტი დათვალიერებისა და სტრიმინგისთვის.

ფუნქციები და მახასიათებლები: შეაფასეთ VPN-ის მიერ შემოთავაზებული დამატებითი ფუნქციები, როგორიცაა „Kill Switch" ფუნქცია, რომელიც სუსტი კავშირის შემთხვევაში, ავტომატურად გამორთავს თქვენს ინტერნეტ-კავშირს, „Split Tunneling" ფუნქცია, რომელიც ინტერნეტ ტრაფიკის მარშრუტირებას ახდენს გაყოფილი გვირაბის ტექნიკის გამოყენებით და ზოგადი მუშაობის ხარისხი.

ღირებულება: შესაძლოა, უფასო VPN-ი მაცდურად გამოიყურებოდეს, თუმცა, ფასიანი სერვისები ხშირად უკეთეს უსაფრთხოებას და შესრულებას უზრუნველყოფენ. აირჩიეთ ისეთი VPN-ი, რომელიც თქვენს ბიუჯეტს შეესაბამება და გაწეული ხარჯისთვის ადეკვატურ სარგებელს გთავაზობთ.

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

1. საჯარო Wi-Fi ქსელების გამოყენება მომხმარებლებს პოტენციური კიბერ შემოჭრის საფრთხის ქვეშ აყენებს, რადგან საჯარო ქსელის თითოეულ მომხმარებელს შეუზღუდავი წვდომა აქვს ქსელში გადაცემულ ინფორმაციაზე.
2. უაღრესად მგრძნობიარე მონაცემებთან მუშაობის დროს, სანდო და არასაჯარო Wi-Fi ქსელზე წვდომის მიღებამდე დაცდა ყველაზე უსაფრთხო არჩევანია.
3. განიხილეთ Hotspot-ის ან VPN-ის გამოყენება.
4. სწორი უსაფრთხოების მეთოდის შერჩევა ინფორმაციის სენსიტიურობისა და გადაუდებლობის ხარისხზეა დამოკიდებული.



შეამოწმეთ თქვენი ცოდნა:

კითხვა 1: რა პოტენციურ რისკებთან არის დაკავშირებული საჯარო Wi-Fi-ს გამოყენება?

ა. ინფორმაციაზე შეზღუდული წვდომა
ბ. გაძლიერებული უსაფრთხოება
გ. კიბერშეტევების წინაშე დაუცველობა
დ. მომხმარებელთა ფიზიკური მდებარეობისთვის თვალის დევნება

როგორ აუმჯობესებს VPN-ი უსაფრთხოებას საჯარო WiFi-ს გამოყენების დროს?

ა. მგრძნობიარე ინფორმაციის გამჟღავნებით
ბ. ონლაინ აქტივობების შეზღუდვით
გ. უსაფრთხო კავშირის დამყარებით
დ. საჯარო ქსელებისთვის გვერდის ავლით

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები

რა საერთო აქვთ თქვენი სახლის გასაღებებსა და პაროლებს?

„პაროლები საცვლებივითაა: მათ ხალხს არ აჩვენებ, ხშირად (ი)ცვლი და არ უზიარებ სხვებს“

კრის პირილო

პროფესიონალური რჩევა:

თავი აარიდეთ სხვადასხვა ანგარიშზე ერთი და იგივე პაროლის გამოყენებას

ერთ მშვენიერ შუადღეს, თბილისის ხალხმრავალ ქუჩებში სეირნობის დროს, ნინო მოულოდნელი განსაცდელის წინაშე აღმოჩნდა - გააცნობიერა, რომ არ იცის სად არის მისი სახლის გასაღები. ნელ-ნელა შფოთვა იგრძნო, რადგან შეეშინდა, რომ მისი ფიზიკური უსაფრთხოება შესაძლოა საფრთხის ქვეშ აღმოჩნდეს. იმის დაშვებით, რომ მისი სახლი ქურდობისათვის ხელმისაწვდომი ადგილი გახდა, ნინო სახლში მშვიდად ვეღარ დაიძინებს. ის სასწრაფოდ უკან მიუყვება გავლილ გზას და ათვალიერებს გარემოს, მაგრამ ვერ ახერხებს გასაღების პოვნას. აცნობიერებს რა საფრთხის სიმძიმეს, სასწრაფოდ უკავშირდება პოლიციას და აცხადებს დაკარგული გასაღების შესახებ, ურეკავს ხელოსანს საკეტის შესაცვლელად და სთხოვს მას გასაღების რამდენიმე ასლის დამზადებას, რათა ერთ-ერთი მათგანი მისთვის სანდო ადამიანთან დატოვოს.

ისევე როგორც ნინოს გასაღებები აღებენ მისი სახლის კარს, პაროლები ციფრულ სამყაროში არსებული ღირებული ნივთების (საბანკო ანგარიშები, ელ.ფოსტა, შეტყობინებები, პირადი ინფორმაცია, სამსახურის მონაცემები, ბენეფიციარები, პირადი შეტყობინებები და ა.შ) გასაღებებს წარმოადგენენ.

Amount of time to crack a password		
7 სიმბოლო		29 მილი წამი
8 სიმბოლო		1-5 საათი
9 სიმბოლო		11 საათიდან -5 დღემდე
10 სიმბოლო		3-4 თვე
11 სიმბოლო		10 წელი
12 სიმბოლო		2 საუკუნე

წყარო 17: რამდენი დრო სჭირდება ჰაკერს პაროლის გასატეხად?

NICK NIGHT | UNSPLASH

სწრაფი გზამკვლევი ძლიერი და დაცული პაროლის შესაქმნელად:

მოერიდეთ გავრცელებულ პაროლებს:
თავი შორს დაიჭირეთ ადვილად გამოსაცნობი პაროლებისაგან, როგორიცაა “password123” ან სხვა გავრცელებული სიტყვები. მეტი დაცულობისთვის შეარჩიეთ უნიკალური კომბინაციები.
კარგი მაგალითი: Tr3ndyP@ssw0rd! (რთული და უნიკალური)
ცუდი მაგალითი: Password123 (მარტივი და ხშირად გამოყენებული)

გამოიყენეთ შერეული სიმბოლოები:
კომბინაციის გასართულებლად, ერთმანეთს შეურიეთ დიდი და პატარა ასოები, რიცხვები და სპეციალური სიმბოლოები.
კარგი მაგალითი: F!reDraGon87#
(მოიცავს მრავალფეროვან სიმბოლოებს)
ცუდი მაგალითი: password1234
(აკლია მრავალფეროვნება და კომპლექსურობა)

პაროლის სიგრძე მნიშვნელოვანია:
შექმენით გრძელი პაროლი, რადგან ისინი უფრო ძლიერი და საიმედოა. რეკომენდებულია მინიმუმ 12 სიმბოლოს გამოყენება.
კარგი მაგალითი: S3cur3L0ngP@ssw0rd!
(გრძელი და კომპლექსური)
ცუდი მაგალითი: ShortPwd!
(ზედმეტად მოკლე ძლიერი დაცვისთვის)

ყველა ანგარიშისთვის სხვადასხვა პაროლი გამოიყენეთ:
თავი აარიდეთ სხვადასხვა ანგარიშზე ერთი და იგივე პაროლის გამოყენებას. სხვადასხვა ანგარიშზე განსხვავებული პაროლების გამოყენება ზრდის უსაფრთხოებას.

მოერიდეთ პირადი ინფორმაციის გამოყენებას:
თავი აარიდეთ პაროლებში პირადი ინფორმაციის გამოყენებას, როგორიცაა სახელები, დაბადების დღეები და მისამართები. ეს ინფორმაცია თავდამსხმელებისთვის ადვილად ხელმისაწვდომია.
კარგი მაგალითი: B3l0v3dPet#R0v3r (მოიცავს პირად ინფორმაციას, თუმცა არაა აშკარა)
ცუდი მაგალითი: JohnsDog123 (პირდაპირ ამჟღავნებს პირად ინფორმაციას)

რეგულარული განახლება:
პერიოდულად შეცვალეთ პაროლები რისკის შესამცირებლად. პაროლების რამდენიმე თვეში ერთხელ განახლების მიზნით, ისარგებლეთ შეხსენების ფუნქციით.

გამოიყენეთ 2FA (ორფაქტორიანი ავტორიზაცია) ან MFA (მრავალფაქტორიანი ავთენტიფიკაცია): ორფაქტორიანი ავტორიზაცია დაცვის დამატებით შრეს ქმნის და მომხმარებლებს იდენტიფიცირების მეორე ფორმას სთხოვს. როგორიცაა, მაგალითად ერთჯერადი კოდის გაგზავნა მობილურ ტელეფონზე.

ეს მნიშვნელოვნად ამცირებს ანგარიშებზე არაავტორიზებული წვდომის მიღებას, იმ შემთხვევაშიც კი, თუკი პაროლი გატეხილია.

გამოიყენეთ პაროლების მენეჯერი: თუკი ბევრი ანგარიში გაქვთ და პაროლების აღრიცხვა გესაჭიროებათ, გამოიყენეთ პაროლების მენეჯერი. გთავაზობთ კიბერ ექსპერტების მიერ რეკომენდებულ რამდენიმე ყველაზე უსაფრთხო და სანდო პაროლების მენეჯერს:

1Password:

ცნობილია ფუნქციების მრავალფეროვნებითა და მარტივი, ინტუიციური დიზაინით.
ექსპერტების რეკომენდაცია: ითვლება საუკეთესო პაროლების მენეჯერად. გვთავაზობს დაბალანსებულ ფუნქციებს, მარტივ გამოყენებას და ხელმისაწვდომობას.

Bitwarden

ღია საწყისი კოდის მქონე პაროლების მენეჯერი აქცენტით უსაფრთხოებაზე.
ექსპერტების რეკომენდაცია: აღიარებულია უსაფრთხოების ზომებით და სხვადასხვა პლატფორმაზე დაყენების შესაძლებლობით.

NordPass

შემუშავებულია NordVPN-ის შემქმნელების მიერ და გვთავაზობს დაცვის ფუნქციების ძლიერ მახასიათებლებს.
ექსპერტების რეკომენდაცია: ერთ-ერთ საუკეთესო არჩევანი 2024 წელს.

განიხილეთ საიდუმლო ფრაზის გამოყენება: საიდუმლო ფრაზა გამოიყენება ავთენტიფიკაციისთვის და წარმოადგენს სიტყვების წყობისგან შემდგარ წინადადებას, რომელიც ტრადიციულ პაროლზე უფრო გრძელი, ადვილად დასამახსოვრებელი და რთულად გასატეხია.
კარგი მაგალითი: PurpleElephant$JumpHigh (გრძელი და დასამახსოვრებელი საიდუმლო ფრაზა)
ცუდი მაგალითი: MyPassword123 (მარტივი და გავრცელებული პაროლის მსგავსი)

პაროლი თუ საიდუმლო ფრაზა?

როგორც წესი, პაროლი მომხმარებლის ავთენტიფიკაციისთვის საჭირო სიმბოლოების კომბინაციაა, რომელიც ასოებს, რიცხვებს და სხვა სიმბოლოებს მოიცავს. სტანდარტულად, ისინი მოკლე და შედარებით კომპლექსურია. მეორე მხრივ, საიდუმლო ფრაზა სიტყვების ან წინადადებების უფრო გრძელი მიმდევრობაა. მათი სიგრძის მიუხედავად, როგორ წესი, საიდუმლო ფრაზების დამახსოვრება უფრო ადვილია.

რომელი უფრო უსაფრთხოა? პაროლისა და საიდუმლო ფრაზის უსაფრთხოება არაერთ ფაქტორზეა დამოკიდებული, მათ შორის, სიგრძესა და კომპლექსურობაზე. როგორც წესი, უფრო გრძელი და რთული პაროლები ან საიდუმლო ფრაზები მეტად უსაფრთხოა. საიდუმლო ფრაზები ხშირად უკეთეს უსაფრთხოებას უზრუნველყოფს მათი სიგრძისა და ენის ბუნებრივი ელემენტების გამოყენების გამო.

სიმბოლოების ოდენობა	მხოლოდ რიცხვები	პატარა ასოები	დიდი და პატარა ასოები	რიცხვები, დიდი და პატარა ასოები	რიცხვები, დიდი და პატარა ასოები, სიმბოლოები
4	მყისიერად	მყისიერად	მყისიერად	მყისიერად	მყისიერად
5	მყისიერად	მყისიერად	მყისიერად	მყისიერად	მყისიერად
6	მყისიერად	მყისიერად	მყისიერად	მყისიერად	მყისიერად
7	მყისიერად	მყისიერად	1 წამი	2 წამი	4 წამი
8	მყისიერად	მყისიერად	28 წამი	2 წუთი	5 წუთი
9	მყისიერად	3 წამი	24 წუთი	2 საათი	6 საათი
10	მყისიერად	1 წუთი	21 საათი	5 დღე	2 კვირა
11	მყისიერად	32 წუთი	1 თვე	10 თვე	3 წელი
12	1 წამი	14 საათი	6 წელი	53 წელი	226 წელი
13	5 წამი	2 კვირა	332 წელი	3 K წელი	15 K წელი
14	52 წამი	1 წელი	17 K წელი	202 K წელი	1 M წელი
15	9 წუთი	27 წელი	898 K წელი	12 M წელი	77 M წელი
16	1 საათი	713 წელი	46 M წელი	779 M წელი	5 BN წელი
17	14 საათი	18K წელი	2 BN წელი	48 BN წელი	380 BN წელი
18	6 დღე	481K წელი	126 BN წელი	2 TN წელი	26 TN წელი

წყარო 18: საკმარისად ძლიერია თქვენი პაროლი?

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

1. სახლის გასაღებების მსგავსად, პაროლებს არსებითი მნიშვნელობა აქვთ თქვენი უსაფრთხოებისთვის. კომპრომისები ამ საკითხთან დაკავშირებით საფრთხეს უქმნის როგორც ფიზიკურ, ისე ციფრულ უსაფრთხოებას.
2. ანგარიშების დასაცავად გამოიყენეთ რთული პაროლები და საიდუმლო ფრაზები. უსაფრთხოების გასაძლიერებლად, შექმენით უნიკალური კომბინაციები, აურიეთ სიმბოლოები და გამოიყენეთ გრძელი პაროლები (რეკომენდებულია მინიმუმ 12 სიმბოლოსგან შემდგარი პაროლის გამოყენება).
3. მიიღეთ უსაფრთხოების დამატებითი ზომები. ორფაქტორიანი ავთენტიფიკაცია (2FA) პაროლებს კიდევ ერთი დამცავი შრით უზრუნველყოფს.

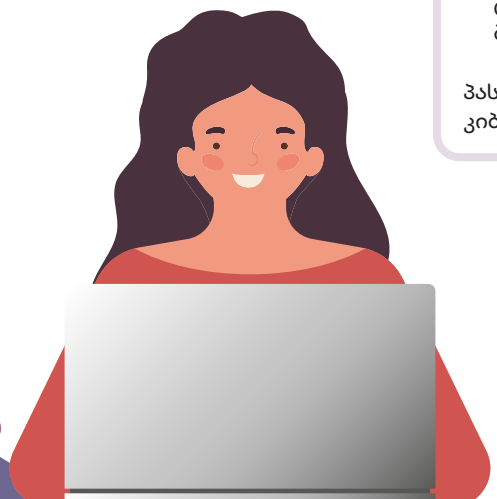
შეამოწმეთ თქვენი ცოდნა:

სცენარი: სალომემ შემაშფოთებელი შეტყობინება მიიღო მის პერსონალურ მონაცემებზე არაავტორიზებული წვდომის შესახებ. შეშინებულმა გააანალიზა, რომ სიტუაციის გამოსასწორებლად და სენსიტიური ინფორმაციის დასაცავად, აუცილებელია სასწრაფოდ მოქმედება.

ტესტის შეკითხვა:
რა ნაბიჯები უნდა გადადგას სალომემ არაავტორიზებული წვდომისა და ინფორმაციის გაჟონვის შესახებ შეტყობინების მიღების შემდეგ?

ა) შეტყობინების იგნორირება, რადგან ის შეიძლება ცრუ განგაში იყოს.
ბ) შეტყობინების ავტორ კომპანიასთან დაკავშირება და ახსნა-განმარტების მოთხოვნა.
გ) გატეხილი ანგარიშის პაროლის შეცვლა და ორფაქტორიანი ავთენტიფიკაციის გააქტიურება.
დ) შეტყობინების სოციალურ მედიაში გაზიარება, პოტენციური რისკების შესახებ სხვების გაფრთხილების მიზნით.

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები



მავნე პროგრამა: ვირუსი, რომელიც ასუსტებს კომპიუტერის იმუნურ სისტემას

ორშაბათი დილაა და ნინო თბილისში ორდღიანი ტრენინგის ჩასატარებლად ემზადება იმ ახალგაზრდა აქტივისტებისთვის, რომლებიც სოციალურ მედიასა და მათ თემებში ქალთა უფლებების ადვოკატირებაზე მუშაობენ. მოულოდნელად, ნინოს მეტოქე გამოუჩნდა – ვირუსი, რომელმაც მის სხეულში შეაღწია და სნეულება, ცხელება და სისუსტე გამოიწვია.

ვირუსის გავრცელებასთან ერთად, ნინოს იმუნური სისტემა მოქმედებას იწყებს. სისხლის თეთრი უჯრედები, მისი სხეულის დამცველები, საფრთხის იდენტიფიცირების და განეიტრალების მიზნით იკრიბებიან. ამასობაში, ნინოს ენერგია სწრაფად ილევა, რაც მისი საკვანძო როლის შესრულების უნარზე აისახება. ნინო იძულებული ხდება გადადოს ტრენინგის ჩატარება მანამ, სანამ მისი იმუნური სისტემა ვირუსის განეიტრალებას მოახერხებს.

მსგავსი პროცესები ვითარდება, როდესაც მავნე პროგრამა თქვენს კომპიუტერში შეღწევას ახერხებს, რისკის ქვეშ აყენებს ფაილებს და აფერხებს სისტემის ფუნქციონირებას.

რა განსხვავებაა მავნე პროგრამასა და ვირუსს შორის?

მავნე პროგრამა ფართო ტერმინია, რომელიც მოიცავს ნებისმიერ მავნე პროგრამულ უზრუნველყოფას, რომელიც შექმნილია კომპიუტერის ან ქსელის დაზიანების მიზნით. იგი მოიცავს სხვადასხვა ტიპებს, როგორიცაა ვირუსები, ტროიანები და გამოსასყიდი პროგრამები. ვირუსი მავნე პროგრამის სპეციფიკურ ტიპს წარმოადგენს, რომელიც ფაილებსა თუ სისტემებზე გავრცელების მიზნით მრავლდება. რომ შევაჯამოთ, ყველა ვირუსი მავნე პროგრამაა, მაგრამ ყველა მავნე პროგრამა ვირუსი არ არის.

ასპექტი	მავნე პროგრამა კომპიუტერში	ვირუსი ადამიანის სხეულში
ძირითადი მახასიათებელი	მავნე პროგრამული უზრუნველყოფა, რომელიც შექმნილია სისტემების დაზიანების ან ექსპლოატირების მიზნით.	ინფექციური აგენტები, რომლებიც იწვევენ დაავადებებს ცოცხალ ორგანიზმებში.
ფორმები	წარმოდგენილია სხვადასხვა ფორმით, მათ შორის ვირუსები, კომპიუტერული ჭიები, ტროიანები და სხვა.	წარმოდგენილია სხვადასხვა დაავადებების გამომწვევი ვირუსების (მაგ. გრიპი) სახით.
გავრცელება	ვრცელდება ინფიცირებული ფაილების, ვებსაიტების ან ჩამოტვირთვების საშუალებით.	ვრცელდება როგორც პირდაპირი კონტაქტით, ისე ჰაერწვეთოვანი გზით.
გამრავლება	კომპიუტერულ სისტემაში მრავლდება შემდგომი გავრცელების მიზნით.	ვირუსის მატარებლის უჯრედებში მრავლდება დაავადების გავრცელების მიზნით.
მიზანი	მონაცემების მოპარვა, სისტემის შეფერხება ან ჯაშუშობა.	სხვადასხვა ხარისხის სიმძიმის დაავადებების გამოწვევა
გამოვლენა	ვლინდება ანტივირუსული პროგრამული უზრუნველყოფისა და კიბერუსაფრთხოების ხელსაწყოების საშუალებით.	ვლინდება ანალიზებით და სამედიცინო გამოკვლევებით.
თავიდან აცილება	თავიდან აცილება შესაძლებელია ანტივირუსის, ფაირვოლებისა და განახლებების გამოყენებით.	თავიდან აცილება შესაძლებელია ვაქცინაციებით, ჰიგიენის დაცვით და ჯანსაღი იმუნიტეტით.
სისტემაზე ზემოქმედება	აფერხებს და არღვევს ოპერაციებს ან აზიანებს მონაცემებს.	იწვევს ავადმყოფობის მსუბუქ და მძიმე სიმპტომებს.
მკურნალობა	საჭიროებს მავნე პროგრამების მოშორების ინსტრუმენტებს და სისტემის აღდგენას.	საჭიროებს სამედიცინო, მედიკამენტურ და მხარდამჭერ მკურნალობას.
ევოლუცია	მუდმივად ვითარდება ახალი სახეობების და ტექნოლოგიების გზით.	ვითარდება მუტაციების გზით, რაც იწვევს ახალი ვირუსის შტამების წარმოქმნას.
წარმოშობა	შემუშავებულია კიბერკრიმინალების ან მავნე ორგანიზაციის მიერ.	ჩნდება ბუნებრივი წყაროებიდან ან შეიძლება იყოს ადამიანის მიერ წარმოებული.

მავნე პროგრამები მავნე პროგრამული უზრუნველყოფის შემოკლებული ფორმაა.

(დიახ, მათაც აქვთ მეტსახელები!)

ეს არის საზიანო პროგრამების კოლექტიური ტერმინი, რომლებიც შექმნილია კომპიუტერების დაზიანების, ინფორმაციის მოპარვის ან ნორმალური ფუნქციონირების შეფერხების მიზნით.

ამ ეტაპზე, შეიძლება ფიქრობთ, რატომ დაესხმიან თავს კიბერ კრიმინალები თქვენ ან თქვენს ორგანიზაციას მავნე პროგრამის გამოყენებით?

1. **პოლიტიკური ჯაშუშობა:** ორგანიზაციების სენსიტიური მონაცემების გამოყენებით, ჰაკერები შეიძლება ჩაერთონ პოლიტიკურ ჯაშუშობაში, იმ ქალების შესახებ ცნობების შეგროვების მიზნით, რომლებიც პოლიტიკურ საქმიანობასა და ადამიანის უფლებების დაცვაში მონაწილეობენ (22).
2. **აქტივიზმის შეფერხება:** მავნე აქტორებმა შეიძლება მიზნად დაისახონ ქალთა უფლებების დამცველი ჯგუფების საქმიანობის შეფერხება, მათი სისტემების მავნე პროგრამით დაინფიცირების გზით. ხსენებულმა შეიძლება ხელი შეუშალოს ორგანიზაციების უნარს, მხარი დაუჭირონ ცვლილებას.
3. **საყრდენი წერტილი უფრო მასშტაბური შეტევებისთვის:** ჰაკერები ხშირად იყენებენ მავნე პროგრამებს საყრდენი წერტილის მოსაპოვებლად. ქსელში შეღწევის შემდეგ, მათ შეუძლიათ წვდომის გაფართოება და უფრო ფართომასშტაბიანი შეტევების განხორციელება, რაც პოტენციურად დააზიანებს ორგანიზაციის მთლიან ინფრასტრუქტურას (23).
4. **პოლიტიკური ან სოციალური ზემოქმედება:** საფრთხის შემქმნელებმა შეიძლება გამოიყენონ მავნე პროგრამა კონკრეტული პოლიტიკური ან სოციალური დღის წესრიგის გასამყარებლად, როგორიცაა დეზინფორმაციის გავრცელება ან ქალთა უფლებების დამცველი ორგანიზაციების საქმიანობის დისკრედიტაცია (24).

სხვადასხვა სახის მავნე პროგრამები არსებობს? დიახ, საკმაოდ ბევრი...

პროგრამა-ჯაშუში (Spyware): როგორც ციფრული ჯაშუშები, ფარულად აკვირდებიან და იპარავენ ინფორმაციას.

რეკლამიანი მავნე პროგრამა (Adware): როგორც გამაღიზიანებელი ამომხტომი მოვაჭრეები, ბომბარდირებას ახდენენ არასასურველი რეკლამებით.

გამოსასყიდი პროგრამა (Ransomware): როგორც ციფრული გამტაცებლები, ბლოკავენ ფაილებს გამოსასყიდის გადახდამდე.

კომპიუტერული ჭია (Worm): როგორც ინფექციების გამავრცელებლები, მრავლდებიან და ბოროტად იყენებენ კიბერ დაუცველობას.

ტროიანი (Trojan): როგორც თაღლითური საჩუქრები, თავს ლეგიტიმურ პროგრამებად ასაღებენ.

კიბერ-ექსპერტების მიერ რეკომენდებული ანტივირუსული, ანტი-ჯაშუშური და ფაირვოლ გადაწყვეტილებები:

Bitdefender

norton

რამდენიმე ფაქტი მავნე პროგრამების შესახებ:

გლობალურად, 2023 წელს ყველა ორგანიზაციის **72,7** პროცენტი გახდა გამოსასყიდი პროგრამის თავდასხმის მსხვერპლი, რაც კიბერუსაფრთხოებაზე მათ მნიშვნელოვან გავლენას ხაზს უსვამს.

2020 წელს, ორგანიზაციების **61**-მა პროცენტმა განიცადა მავნე პროგრამების გავრცელება ერთი თანამშრომლიდან მეორეზე; 2021 წლისთვის ეს რიცხვი **7** პროცენტით გაიზარდა, რაც ხაზს უსვამს მავნე პროგრამების ინციდენტების მზარდ სიხშირეს.

რეკლამიანმა მავნე პროგრამამ (Adware) 2022 წელს აღმოჩენილი მობილური საფრთხის **25,28** პროცენტი შეადგინა, რაც მავნე პროგრამების სხვადასხვა სახეებს შორის, მის უპირატესობაზე მიანიშნებს.

წყარო: 19 კიბერუსაფრთხოების ძირითადი სტატისტიკური მონაცემები 2024 წლისთვის

წყარო: 20 მავნე პროგრამული უზრუნველყოფის სტატისტიკური მონაცემები და ფაქტები 2024 წლისთვის

წყარო: 21 2023 წლის ყველაზე მნიშვნელოვანი სტატისტიკური მონაცემების მიმოხილვა

რა არის ფაირვოლი (FIREWALL)?

ფაირვოლი თქვენი კომპიუტერის ქსელის დარაჯია:

- აკვირდება და აკონტროლებს შემომავალ და გამავალ ტრაფიკს. ის დამცავი ბარიერის როლს ასრულებს.
- ატარებს კარგ მონაცემებს და ბლოკავს ცუდს, როგორიცაა კიბერ საფრთხეები.
- შეიძლება იყოს აპარატული ან პროგრამული უზრუნველყოფა და გადამწყვეტ როლს თამაშობს უსაფრთხო ონლაინ გარემოს შენარჩუნებაში.

ყურადღების ცენტრში:

როგორ დავიცვათ თავი (კომპიუტერები) მავნე პროგრამებისგან?

ძლიერი პაროლების გამოყენებისა და საეჭვო ბმულებზე გადასვლის თავიდან აცილების გარდა, კიდევ რამდენიმე მნიშვნელოვან რჩევას გთავაზობთ:

- თქვენს კომპიუტერებზე დააყენეთ სანდო ანტივირუსული და ანტი-ჯაშუშური პროგრამები მავნე პროგრამების აღმოსაჩენად და აღმოსაფხვრელად.
- მუდმივად განაახლეთ პროგრამული უზრუნველყოფა, მათ შორის ოპერაციული სისტემები, აპლიკაციები და ანტივირუსული პროგრამები.
- გამოიყენეთ ფაირვოლი (Firewall), როგორც დამატებითი ბარიერი მავნე პროგრამების წინააღმდეგ, რათა აკონტროლოთ შემომავალი და გამავალი ქსელის ტრაფიკი.

შეამოწმეთ თქვენი ცოდნა:

კითხვა 1: რა არის ჯაშუშური პროგრამის მთავარი მიზანი?

ა) სისტემის მუშაობის გაუმჯობესება
ბ) ინფორმაციაზე თვალთვალი და მისი მოპარვა
გ) ფაილების დაბლოკვა გამოსასყიდის გადახდამდე
დ) ინფექციების გავრცელება და გამრავლება

კითხვა 2: მავნე პროგრამების გამოყენებით, რა მიზნებით შეიძლება ჩაერთონ კიბერკრიმინალები პოლიტიკურ ჯაშუშობაში?

ა) სისტემის მუშაობის გაუმჯობესება
ბ) აქტივიზმის შეფერხება
გ) უფრო მასშტაბური შეტევებისთვის საყრდენი წერტილის მოპოვება
დ) კონკრეტული პოლიტიკური ან სოციალური დღის წესრიგის გამყარება

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

ნინოს ბრძოლა ვირუსთან ზუსტად ასახავს მავნე პროგრამის ზემოქმედებას კომპიუტერებზე, რომელიც ოპერაციებს და ფუნქციონირებას აფერხებს. მავნე პროგრამა ზოგადი ტერმინია, რომელიც მავნე პროგრამული უზრუნველყოფის სხვადასხვა ფორმებს მოიცავს.

კიბერკრიმინალები თავს ესხმიან აქტივისტებს მავნე პროგრამით სხვადასხვა მიზეზის გამო, მათ შორის პოლიტიკური ჯაშუშობა, აქტივიზმის შეფერხება, კონკრეტული პოლიტიკური და სოციალური დღის წესრიგის გამყარება და უფრო მასშტაბური შეტევებისთვის საყრდენი წერტილის მოპოვება.

დაიცავით უსაფრთხოება ანტივირუსული და ანტი-ჯაშუშური პროგრამების დაყენებით. რეგულარულად განაახლეთ პროგრამული უზრუნველყოფა და გამოიყენეთ ფაირვოლი.

დაიცავით თქვენი მოწყობილობები, ორგანიზაცია და ბენეფიციარები

კიბერუსაფრთხოების სამყაროში თქვენი მოგზაურობა შეიძლება გამოწვევებით სავსე აღმოჩნდეს. ჩვევების შეცვლას გარკვეული დრო და ძალისხმევა სჭირდება, თუმცა სენსიტიური ინფორმაციის, თქვენი კოლეგებისა და რაც ყველაზე მთავარია, თქვენი ბენეფიციარების დასაცავად არსებითად მნიშვნელოვანია.

მოცემული გზამკვლევი მოგაწვდით ინფორმაციას იმ ნაბიჯების შესახებ, რომლებიც მოწყობილობების დაცვაში, ცნობიერების ამაღლებასა და ორგანიზაციის კიბერუსაფრთხოების გაძლიერებაში დაგეხმარებათ.

ნაბიჯ-ნაბიჯ შევცვალოთ კიბერ ჩვევები

1. თანამშრომლების ტრენინგი:

- ჩაატარეთ კიბერუსაფრთხოების შესახებ ცნობიერების ასამაღლებელი ტრენინგები, რათა თანამშრომლებს გააცნოთ ინფორმაცია ძირითადი საფრთხეების, ფიშინგის თავდასხმების და ინტერნეტის უსაფრთხოდ გამოყენების მნიშვნელობის შესახებ.
- დაიწყეთ კიბერუსაფრთხოების ძირითადი ცნებებით, სანამ უფრო კომპლექსურ საკითხებს ჩაუღრმავდებით.

2. რეგულარული გამეორება:

- თანამშრომლებისთვის დაგეგმეთ განმეორებითი სესიები არსებული ცოდნის განსამტკიცებლად და საფრთხეების შესახებ განახლებული ინფორმაციის მისაწოდებლად.
- წაახალისეთ ღია კომუნიკაცია, მიეცით თანამშრომლებს სირთულეების გაზიარების და შეკითხვების დასმის შესაძლებლობა.

3. ეტაპობრივი დანერგვა:

- დანერგეთ კიბერუსაფრთხოების ზომები ეტაპობრივად, რათა თავიდან აიცილოთ თანამშრომლების დაბნევა.
- დაიწყეთ საბაზისო უნარებით, როგორიცაა ძლიერი პაროლების გამოყენება და თანდათანობით შემოიტანეთ უფრო კომპლექსური საკითხები.

> კიბერუსაფრთხოების ტრენინგი ეფექტურად ჩაითვლება, თუ ის ქცევის შეცვლას გამოიწვევს

ქცევითი ცვლილებები კიბერუსაფრთხოების გასაძლიერებლად

ტექნიკური ზომების გარდა, ქცევითი ცვლილებების ხელშეწყობა სასიცოცხლოდ მნიშვნელოვანია კიბერ მდგრადობისთვის.

1. ინტერნეტის უსაფრთხო დათვალიერების ჩვევები

- ურჩიეთ თანამშრომლებს, რომ გულდასმით დააკვირდნენ URL-ებს, მოერიდონ საეჭვო ბმულებზე გადასვლას და შეამოწმონ ვებსაიტების ლეგიტიმურობა.
- დანერგეთ ვებსაიტების ფილტრაციის ინსტრუმენტები მავნე ვებსაიტებზე წვდომის შესაზღუდად.

2. ორფაქტორიანი ავთენტიფიკაცია (2FA)

- წაახალისეთ ორფაქტორიანი ავტორიზაციის გამოყენება ანგარიშებისა და სისტემის დაცვის დამატებით შრის შესაქმნელად.
- დანერგეთ ბიომეტრიული ავთენტიფიკაცია უსაფრთხოების დამატებითი ზომებისთვის.

3. ინციდენტების შეტყობინების კულტურა

- წაახალისეთ კულტურა, რომელშიც თანამშრომლები შეძლებენ ნებისმიერი საეჭვო აქტივობის ან უსაფრთხოების ინციდენტის დაუყოვნებლივ შეტყობინებას.
- დააწესეთ უსაფრთხოების ინციდენტებზე რეაგირების მკაფიო გეგმა აღმოჩენილი პრობლემების ეფექტური გადაწყვეტისთვის.

კიბერუსაფრთხოებისთვის პრიორიტეტის მინიჭებით, ქალთა უფლებების დამცველი ორგანიზაციები შეძლებენ როგორც კიბერუსაფრთხოების გაძლიერებას, ასევე თავიანთი მნიშვნელოვანი საქმიანობის დაცვას. სწავლების, ეტაპობრივი დანერგვისა და ქცევითი ცვლილებების ხელშეწყობის კომბინაცია, მდგრადი და უსაფრთხო კიბერ გარემოს შექმნას უზრუნველყოფს.

ANRAS VAS | UNSPLASH

კიბერუსაფრთხოების ზომების დანერგვა ორგანიზაციულ დონეზე

1. ანტივირუსული პროგრამების დაყენება
- გამოიყენეთ სანდო ანტივირუსული პროგრამა მავნე საფრთხის აღმოსაჩენად და აღმოსაფხვრელად.
- რეგულარულად განაახლეთ ანტივირუსული პროგრამის მონაცემთა ბაზები, რათა დაცული იყოთ უახლესი საფრთხეებისგან.

2. პროგრამული და აპარატული უზრუნველყოფის რეგულარული განახლებები
- რეგულარულად განაახლეთ ოპერაციული სისტემები და აპლიკაციები სისუსტეების აღმოსაფხვრელად.
- შეძლებისდაგვარად გააქტიურეთ ავტომატური განახლებები, რათა უზრუნველყოთ დროული დაცვა ნაცნობი ექსპლუატატორებისგან.
- დარწმუნდით, რომ აპარატული უზრუნველყოფის ყველა ელემენტს, მათ შორის მარშრუტიზატორებსა და ნივთების ინტერნეტის (IoT) მოწყობილობებს, აქვს პროგრამული უზრუნველყოფის უახლესი განახლებები, უსაფრთხოების პრობლემების გადასაჭრელად.

3. გამოიყენეთ ფაირვოლები (Firewalls)
- გამოიყენეთ ფაირვოლები როგორც ცალკეულ მოწყობილობებზე, ასევე ქსელის ინფრასტრუქტურაზე.
- დააყენეთ ფაირვოლები შემომავალი და გამავალი ქსელის ტრაფიკის მონიტორინგისა და კონტროლისთვის, საერთო უსაფრთხოების გაძლიერების მიზნით.

4. თანამშრომლებისთვის წვდომის ნებართვების რეგულირება
- დანერგეთ მინიმალური პრივილეგიების პრინციპი და თანამშრომლებს მიანიჭეთ წვდომა მხოლოდ მათი საქმიანობისთვის აუცილებელ ინფორმაციაზე.
- რეგულარულად განაახლეთ წვდომის ნებართვები, რათა ისინი თანამშრომლების როლებთან და ორგანიზაციულ ცვლილებებთან შესაბამისობაში იყოს.

5. გამოიყენეთ ინფორმაციის დაშიფვრა
- სენსიტიური ინფორმაციისა და მონაცემების გასაზიარებლად წაახალისეთ დაშიფვრის გამოყენება.
- კონფიდენციალური საუბრებისთვის გამოიყენეთ გამჭოლი (end-to-end) შიფრის მქონე პლატფორმები.

6. რეგულარული სარეზერვო ასლების მომზადება (backup)
- ხაზი გაუსვით მონაცემთა რეგულარული სარეზერვო ასლების მომზადების მნიშვნელობას გამოსასყიდი პროგრამის შეტევების ან მონაცემთა დაკარგვის უარყოფითი გავლენის შესამცირებლად.
- სარეზერვო ასლები შეინახეთ დაცულად, სასურველია ავტონომიურ ან „ქლაუდ“ სერვერზე და პერიოდულად შეამოწმეთ მონაცემების აღდგენის ფუნქციები.

შეამოწმეთ თქვენი ცოდნა

კითხვა 1: რა არის კიბერუსაფრთხოების ტრენინგის მთავარი მიზანი?

ა) მოწყობილობის ვიზუალური მხარის გაუმჯობესება
ბ) ქცევითი ცვლილებების განხორციელება
გ) კიბერუსაფრთხოების ზომების უგულებელყოფა
დ) მხოლოდ რთულ გადაწყვეტილებებზე ორიენტირება

კითხვა 2: რა არის რეკომენდებული მიდგომა ორგანიზაციულ დონეზე კიბერუსაფრთხოების ზომების დასანერგად?

ა) გაძლიერებული ზომების დაუყოვნებელი განხორციელება
ბ) კიბერუსაფრთხოების ზომების შემთხვევითობის პრინციპით დანერგვა
გ) ფუნდამენტური საკითხებით დაწყება და კიბერუსაფრთხოების ზომების ეტაპობრივად დანერგვა
დ) კიბერუსაფრთხოების დაფუძნება მხოლოდ თანამშრომლებისთვის წვდომის ნებართვების რეგულირებაზე

კითხვა 3: კიბერუსაფრთხოების რომელი ზომა გულისხმობს თანამშრომლებისთვის მხოლოდ მათი როლის შესასრულებლად აუცილებელ ინფორმაციაზე წვდომის დაშვებას?

ა) დაშიფვრა
ბ) ფაირვოლები
გ) რეგულარული სარეზერვო ასლების მომზადება (backup)
დ) წვდომის ნებართვების რეგულირება

პასუხები შეგიძლიათ იხილოთ ბოლო თავში: თქვენი კიბერ პასუხები

თუკი, ამ სექციაში მოწოდებული ინფორმაციიდან მხოლოდ რამდენიმეზე გაამახვილებთ ყურადღებას, მაშინ გახსოვდეთ, რომ:

1. პრიორიტეტი მიანიჭეთ კიბერუსაფრთხოებას: გააცნობიერეთ კიბერუსაფრთხოებისკენ მიმავალი გზის სირთულე და ქცევითი ცვლილებების აუცილებლობა სენსიტიური ინფორმაციის დასაცავად.
2. ქმედითი ტრენინგები: დარწმუნდით, რომ კიბერუსაფრთხოების ტრენინგის შედეგად თანამშრომლების ამაღლებულ ცნობიერებას და შესაბამის ქცევით ცვლილებებს აღწევთ. დაიწყეთ კიბერუსაფრთხოების ძირითადი ცნებებით და დაგეგმეთ რეგულარული განმეორებითი სესიები მიღებული ცოდნის განსამტკიცებლად.
3. ეტაპობრივი დანერგვა: კიბერუსაფრთხოების ზომები ეტაპობრივად დანერგეთ ორგანიზაციულ დონეზე. დაიწყეთ ისეთი ფუნდამენტური ნაბიჯებით, როგორიც ანტივირუსის დაყენებაა და ნელ-ნელა უფრო მაღალ საფეხურებზე გადადით.
4. ტექნიკური ზომების მიღება: უზრუნველყავით ანტივირუსული პროგრამული უზრუნველყოფა, რეგულარული განახლებები, ფაირვოლები და დაშიფვრა როგორც ინდივიდუალური მოწყობილობებისთვის, ასევე ქსელის ინფრასტრუქტურისთვის.
5. ქცევითი ცვლილებები: ხელი შეუწყვეთ გაძლიერებული კიბერუსაფრთხოების კულტურის, ინტერნეტის უსაფრთხო დათვალიერების ჩვევების, ორფაქტორიანი ავთენტიფიკაციის გამოყენების და ინციდენტების დროული შეტყობინების დანერგვას.

სიტუაციური სავარჯიშო: ფიშინგის სიმულაცია და საპასუხო რეაგირება

გაითამაშეთ თანამშრომლებზე მიმართული ფიშინგის შეტევა, რათა შეაფასოთ კიბერ საფრთხის აღმოჩენის, სამოქმედო ნაბიჯების თანმიმდევრობის განსაზღვრის და შესაბამისი რეაგირების ორგანიზაციული უნარები.

სავარჯიშოს ნაბიჯები:

1. ფიშინგის ელ. ფოსტის სიმულაცია
- შემთხვევითობის პრინციპით აირჩიეთ თანამშრომლები და გაუგზავნეთ მათ ფიშინგის რეალისტური ელ.ფოსტა.
- შექმენით ფიშინგის ტაქტიკებზე მიმსგავსებული რეალისტური სცენარები გადაუდებელი მოთხოვნების, მიმზიდველი შეთავაზებების ან შენიღბული შიდა კომუნიკაციების გამოყენებით.

2. თანამშრომლების რეაგირება:
- დააკვირდით თანამშრომლების რეაგირებას ფიშინგის ელ. ფოსტაზე.
- შეაფასეთ, რამდენად მოახერხებენ ფიშინგის მცდელობის ამოცნობას, მოახერხებენ ინციდენტის დაუყოვნებლივ შეტყობინებას თუ გახდებიან თავდასხმის მსხვერპლი.

3. უსაფრთხოების გუნდისთვის შეტყობინება:
- აცნობეთ კიბერუსაფრთხოების ჯგუფს სიმულირებული ფიშინგის შეტევის შესახებ.
- შეაფასეთ გუნდის რეაგირების დრო და ეფექტურობა ფიშინგის მცდელობის გაანალიზების და დადასტურების პროცესში.

4. ინციდენტზე რეაგირების პრიორიტეტები:
- ფიშინგის შეტევის სიმძიმის მიხედვით, თანამშრომლებმა უნდა განსაზღვრონ რეაგირების ნაბიჯების პრიორიტეტები.
- შეამოწმეთ ორგანიზაციის მიერ პრიორიტეტების განსაზღვრის და რესურსების ეფექტურად განაწილების უნარები.

5. უკუკავშირი და ტრენინგი:
- შეატყობინეთ თანამშრომლებს გათამაშებული ინციდენტის შესახებ და ხაზი გაუსვით ფიშინგის საფრთხისადმი რეზისტენტულობის მნიშვნელობას.
- დაგეგმეთ მიზნობრივი ტრენინგი ფიშინგის მცდელობების ამოცნობისა და შეტყობინების შესახებ.

6. სავარჯიშოს შემდგომი ანალიზი:
- გაანალიზეთ სავარჯიშო დეტალურად და გამოავლინეთ ადგილები, რომლებიც გაუმჯობესებას საჭიროებს.
- შეაფასეთ ორგანიზაციის კიბერუსაფრთხოების ტრენინგის ეფექტურობა და შესაბამისად დაადგინეთ პრიორიტეტები.

კიბერუსაფრთხოებაში, შეგიძლიათ გქონდეთ საუკეთესო დაცვა (ანტივირუსი, VPN და სხვა) და ეს მაინც არ აღმოჩნდეს საკმარისი. ყველაზე სუსტი რგოლი ადამიანია. ერთმა ადამიანურმა შეცდომამ შეიძლება უსაფრთხოების სისტემის სრული კოლაფსი გამოიწვიოს

დავით ღონღაძე,
კიბერუსაფრთხოების ექსპერტი.

რამდენიმე სიტყვა გზამკვლევის დასასრულს

კიბერ მდგრადობის გზამკვლევის დასასრულს, რომელიც საქართველოში ქალთა უფლებების დამცველი ორგანიზაციების საჭიროებებზეა მორგებული, ნათელი უნდა იყოს ციფრულ უსაფრთხოებასა და ადამიანის უფლებების ადვოკატირებას შორის არსებული მკაფიო თანაკვეთა. სენსიტიური ინფორმაციისა და ციფრული აქტივების დაცვა არ მხოლოდ საუკეთესო პრაქტიკას, არამედ ადამიანის უფლებების დაცვის აუცილებელ წინაპირობას წარმოადგენს.

კიბერ საფრთხეების განვითარებადი გარემო ქალთა უფლებების დამცველ ორგანიზაციებს ქცევის პარადიგმაში განსახორციელებელი ცვლილებების აუცილებლობისკენ მოუწოდებს. კიბერუსაფრთხოების დაცვის მიზნით მიღებული მტკიცე ზომები, რომელიც რეალურ დროში მონიტორინგს და პროაქტიულ გადაწყვეტილებებს მოიცავს, არსებითია ციფრული ინფრასტრუქტურის გასაძლიერებლად პოტენციური რისკების წინააღმდეგ.

იდეალურ სამყაროში, ნინოსა და სალომეს მსგავს ადამიანებს მოსალოდნელი კიბერ საფრთხეების მუდმივი შიშის გარეშე, სრულად შეეძლოთ მიეძღვნათ საკუთარი თავები ქალთა უფლებების ადვოკატირებისთვის, სამოქალაქო აქტივიზმისთვის და ტრენინგებისთვის. თუმცა, არსებული რეალობა კიბერუსაფრთხოების კუთხით ცვლილებების გატარების და ორგანიზაციულ დონეზე უფრო უსაფრთხო პრაქტიკის დანერგვის პარალელურ ადვოკატირებას მოითხოვს. წარმოიდგინეთ, როგორ ხვდებიან სალომე და ნინო ერთმანეთს საყვარელ რესტორანში, რთული სამუშაო კვირის ბოლოს. საფუძვლიანი კიბერ შეფასების ჩატარების და კიბერუსაფრთხოების პრიორიტეტული ღონისძიებების შესახებ მიღებული ტრენინგის შედეგად, მათ, როგორც თავიანთი გუნდის წევრების, ისე ბენეფიციარების დაცვის თავდაჯერებულობა აქვთ.

ეს გზამკვლევი არ არის გამიზნული შიშის ჩასანერგად; ჰირიქით, ის წარმოადგენს პრაქტიკულ რესურსს, რომელიც საქართველოში ქალთა უფლებების დამცველ ორგანიზაციებს ციფრულ გარემოში უსაფრთხო ნავიგაციისთვის აუცილებელი ცოდნით და ინსტრუმენტებით ამარაგებს, რათა მათ გენდერული თანასწორობის და ადამიანის უფლებების დაცვის ცენტრალურ მისიაზე მოახდინონ კონცენტრირება.

SINCERLEY MEDIA | UNSPLASH

თქვენი კიბერ პასუხები

თავი: მართლა სამიზნე ვარ?

პასუხი: სწორი პასუხია ა) მიზნობრივი შეტევა მისი ინფორმაციის მოსაპარად
ნინოს ფიშინგის ელექტრონული წერილი იმ ორგანიზაციის სახელით გაუგზავნეს, რომელთანაც თანამშრომლობს. ხსენებული მიუთითებს მიზნობრივ შეტევაზე, რადგან ჰაკერებმა ჩაატარეს წინასწარი მოკვლევა და გამიზნულად შეარჩიეს ის ორგანიზაცია, რომელსაც ნინო ენდობა. მონაცემების განახლების მოთხოვნის გზით, ისინი მომხმარებლის სახელის და პაროლის მოპარვას და ანგარიშების გატეხას ისახავდნენ მიზნად.

თავი: ინტერნეტის უსაფრთხოდ გამოყენება: ხალხმრავალ ქუჩაზე გახსნილი ჩანთით ივლიდით?

სწორი პასუხებია 1, 2, 4, 5, 6, 7. ერთადერთი არასწორი პასუხია 3.
მიუხედავად იმისა, რომ ელ. ფოსტა სათაურით „სიახლეების გამოწერის დადასტურება“ შეიძლება იყოს ფიშინგის ელ. ფოსტის სათაური, ყველა სხვა სათაურს სასწრაფოების შეგრძნება ახლავს და დაუყოვნებლივი ქმედების გამოსაწვევად იყენებს შიშს. ჰაკერები ხშირად მიმართავენ ემოციური მანიპულირების ტაქტიკებს, რათა მოტყუების გზით გადაიყვანონ ინდივიდები ფიშინგის ელ.ფოსტის ბმულებზე.

თავი: საჯარო Wi-Fi: კიბერ კრიმინალების თავშესაფარი

პირველ კითხვაზე პასუხი არის გ) კიბერშეტევების წინაშე დაუცველობა
ყველაზე მნიშვნელოვანი რისკი, რომელსაც საჯარო Wi-Fi ქსელების გამოყენება ქმნის, არის კიბერშეტევების წინაშე დაუცველობა. ზოგიერთ შემთხვევაში, ეს დაუცველი მდგომარეობა კიბერკრიმინალებს თქვენი ფიზიკური მდებარეობის თვალთვალის შესაძლებლობას აძლევს.

მეორე კითხვაზე პასუხი არის გ) უსაფრთხო კავშირის დამყარებით
VPN-ი აუმჯობესებს დაცულობას საჯარო Wi-Fi-ს გამოყენების დროს. ის გადაამისამართებს თქვენს ინტერნეტ კავშირს კერძო სერვერის მეშვეობით, რაც მიუწვდომელს ხდის თქვენს რეალურ IP მისამართს და მალავს ონლაინ აქტივობას.

თავი: რა საერთო აქვთ თქვენი სახლის გასაღებებსა და პაროლებს?

სიტუაციური სავარჯიშოს კითხვაზე სწორი პასუხი არის გ) გატეხილი ანგარიშის პაროლის შეცვლა და ორფაქტორიანი ავთენტიფიკაციის გააქტიურება.
თუ მისი პაროლი კომპრომეტირებულია მონაცემთა გაჟონვის შედეგად, ეს ნიშნავს, რომ კიბერ ჰაკერებს აქვთ წვდომა მის მომხმარებლის სახელსა და პაროლზე. სალომემ სასწრაფოდ უნდა შეცვალოს გატეხილი ანგარიშის პაროლი და დამატებითი დაცვის უზრუნველსაყოფად, გააააქტიუროს ორფაქტორიანი ავთენტიფიკაცია.

თავი: მავნე პროგრამა: ვირუსი, რომელიც ასუსტებს კომპიუტერის იმუნურ სისტემას

პირველ კითხვაზე პასუხი არის ბ) ინფორმაციაზე თვალთვალი და მისი მოპარვა
ციფრული აგენტების მსგავსად, ჯაშუშური პროგრამების მთავარი მიზანი ინფორმაციაზე ფარული თვალთვალი და მისი მოპარვაა.

მეორე კითხვაზე პასუხი არის ბ) აქტივიზმის შეფერხება
ჰაკერები შეიძლება ჩაერთონ პოლიტიკურ ჯაშუშობაში და აქტივისტების, მშვიდობის მშენებლებისა და ორგანიზაციების შესახებ მოპოვებული სენსიტიური მონაცემები აქტივიზმის შეფერხების მიზნით გამოიყენონ.

თავი: დაიცავით თქვენი მოწყობილობები, ორგანიზაცია და ბენეფიციარები

პირველ კითხვაზე პასუხი არის ბ) ქცევითი ცვლილებების განხორციელება
ნებისმიერი კიბერუსაფრთხოების ტრენინგის უპირველესი მიზანია ადამიანებში ქცევითი ცვლილებების განხორციელების წახალისება, ორგანიზაციის თანამშრომლებისთვის უფრო უსაფრთხო სამუშაო გარემოს შექმნის მიზნით.

მეორე კითხვაზე პასუხი არის გ) ფუნდამენტური საკითხებით დაწყება და კიბერუსაფრთხოების ზომების ეტაპობრივად დანერგვა
რეკომენდებულია კიბერუსაფრთხოების ფუნდამენტური საკითხებით დაწყება, როგორიცაა ინტერნეტის უსაფრთხოდ დათვალიერება და ფიშინგ ელ. ფოსტის ამოცნობა. ამის შემდეგ, შეგიძლიათ გადახვიდეთ დაშიფრულ ელ. წერილებზე, ფაირვოლებზე, VPN-ებზე და სხვა უფრო კომპლექსურ თემებზე.

მესამე კითხვაზე პასუხი არის დ) წვდომის ნებართვების რეგულირება

წყაროები

https://www.gisreportsonline.com/r/georgia-russia-west/

https://www.ui.se/forskning/centrum-for-osteuropastudier/sceeus-commentary/russias-war-on-ukraine--consequences-for-georgia-and-moldova/

https://www.csis.org/analysis/georgia-civil-society-wins-against-russia-style-foreign-agents-bill

https://www.politico.eu/article/russia-vladimir-putin-style-foreign-agent-bill-in-georgia-threatens-civil-society/

https://www.reuters.com/world/europe/parliament-georgia-gives-initial-approval-foreign-agents-law-2023-03-07/

https://blogs.lse.ac.uk/humanrights/2023/07/17/failed-attempt-of-the-georgian-government-to-silence-civil-society-organisations/

https://gfsis.org.ge/blog/view/996

https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

https://www.pentasecurity.com/blog/can-learn-georgias-massive-cyberattack-better/

https://www.justice.gov/usao-ndga/pr/georgia-cyber-fraud-task-force-marks-two-years-addressing-laundering-cyber-enabled

https://civil.ge/archives/446772

https://civil.ge/archives/582011

https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf

https://georgia.unwomen.org/en/digital-library/publications/2018/03/national-study-on-violence-against-women-in-georgia-2017

https://data.unwomen.org/features/georgia-violence-against-women-study-ushers-countrys-first-sexual-harassment-law

https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations

https://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma

https://www.amnesty.org/en/latest/campaigns/2015/08/how-governments-are-using-spyware-to-attack-free-speech/

https://tech.co/password-managers/how-long-hacker-crack-password#:~:text=A%2010%2Ddigit%20password%20that,hacker%20up%20to%20two%20weeks

https://www.verveit.com/blog/is-your-password-strong-enough/

https://www.cobalt.io/blog/cybersecurity-statistics-2024

https://www.comparitech.com/antivirus/malware-statistics-facts/

https://terranovasecurity.com/blog/cyber-security-statistics/

https://www.linkedin.com/pulse/breaking-down-tactics-used-hackers-exploit-womens-rights-middle

https://www.sciencedirect.com/science/article/pii/S245195882200001X

https://www.ibm.com/topics/threat-actor

INSTITUTE FOR
WAR & PEACE REPORTING

iwpr.net

IWPR United Kingdom
48 Gray's Inn Road,
London WC1X 8LT
Tel +44 (0)20 7831 1030

IWPR United States
1156 15th Street NW Suite 329,
Washington, DC 20005
Tel +1 202 393 5641

IWPR Netherlands
iwpr-nl@iwpr.net