# კიბერუსაფრთხოება:

## გარემოს ანალიზი და პრევენციული მექანიზმები


# კიბერუსაფრთხოება:

## გარემოს ანალიზი და პრევენციული მექანიზმები

ავტორები: დავით შავგულიძე და გიორგი გურგენიძე

2023 წელი

# სახელმძღვანელოს შესახებ

წინამდებარე სახელმძღვანელო მომზადდა საქართველოს ინფორმაციის და ტექნოლოგიების ანალიზის ცენტრის (GITAC) მიერ საქართველოს სტრატეგიის და განვითარების ცენტრის (GCSD) დაკვეთით.

პროექტი "ინფორმირებული თემები მედეგი საზოგადოებისთვის" - აშშ-ის საელჩოს დემოკრატიის კომისიის მცირე გრანტების პროგრამის მხარდაჭერით ხორციელდება, რომლის მიზანია ხელი შეუწყოს საქართველოში ეთნიკური უმცირესობებით და იძულებით გადაადგილებული პირებით მჭიდროდ დასახლებულ რეგიონებში (სამეგრელო, სამცხეჯავახეთი, ქვემო ქართლი, შიდა ქართლი) მცხოვრები საზოგადოების მედეგობის გაძლიერებას კიბერ და დეზინფორმაციული საფრთხეების მიმართ.

სახელმძღვანელოს მომზადებისას გამოყენებული იქნა საჯაროდ ხელმისაწვდომი, არაკომერციული სახის ლიტერატურა. სახელმძღვანელოს ძირითად მეთოდოლოგიურ ბაზას წარმოადგენს:

- აშშ-ს კიბერუსაფრთხოებისა და კრიტიკული ინფრასტრუქტურის სააგენტოს (US CISA) სახელმძღვანელოები;
- აშშ-ს სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (US NIST) სახელმძღვანელოები და ტერმინთა განმარტებები;
- დიდი ბრიტანეთის ეროვნული კიბერუსაფრთხოების ცენტრის (UK NCSC) სახელმძღვანელოები;
- კანადის კიბერუსაფრთხოების ცენტრის (Canadian Centre for Cybersecurity) სახელმძღვანელოები;
- ევროპის საბჭოს (CoE) სახელმძღვანელოები;

სახელმძღვანელოს მომზადებისას ასევე გამოყენებული იქნა საქართველოს მოქმედი კანონმდებლობა ინფორმაციული უსაფრთხოებისა და პერსონალურ მონაცემთა დაცვის შესახებ.

სახელმძღვანელოში მოცემული კიბერუსაფრთხოების კონტროლები და რჩევები უზრუნველყოფს კიბერრისკების შემცირებასა და საფრთხეების მართვას. მნიშვნელოვანია, რომ სახელმძღვანელო არ იძლევა გარანტიას ყველა სახის კიბერშეტევისგან თავის დასაცავად, თუმცა ქვემოთ მოყვანილი ნაბიჯები მნიშვნელოვნად შეამცირებს საფრთხის შანსს, რათა თქვენ, თქვენი ბიზნესი ან ორგანიზაცია კიბერდანაშაულის მსხვერპლი არ გახდეს.

სახელმძღვანელოს შინაარსზე პასუხისმგებელნი არიან მხოლოდ მისი ავტორები და არა, პროცესში ჩართული, რომელიმე სხვა მხარე. GCSD-ის წერილობითი თანხმობის გარეშე დოკუმენტის არცერთი ნაწილი არ შეიძლება გადაიბეჭდოს ნებისმიერი, მათ შორის ელექტრონული ან მექანიკური ფორმით.

საქართველოს სტრატეგიის და განვითარების ცენტრის შესახებ

GCSD არის მიუკერძოებელი და ნეიტრალური არასამთავრობო ორგანიზაცია, რომლის ღირებულებები ეფუძნება თანასწორობის, ადამიანის თავისუფლების, პატივისცემის, ანგარიშვალდებულებისა და გამჭირვალობის პრინციპებს. ცენტრის ძირითადი მიზნებია: საქართველოს ეროვნული უსაფრთხოების უზრუნველყოფის ხელშეწყობა; ქვეყნის ეფექტიანი და დემოკრატიული მართვის პრინციპების განმტკიცება; მისი ევროპული და ევრო-ატლანტიკური ინტეგრაციის მხარდაჭერა და ქვეყნის მდგრადი განვითარების პირობების შექმნა.

მეტი ინფორმაციისთვის ეწვიეთ: [https://www.gcsd.org.ge/ge](https://www.gcsd.org.ge/ge)

# სარჩევი

# ტერმინთა განმარტება

**კიბერუსაფრთხოება** - წარმოადგენს ქსელების, მოწყობილობებისა და მონაცემების დაცვას ეკანონო ქმედებისგან, წვდომისგან ან კრიმინალური გამოყენებისგან, რომელიც ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის ეზრუნველყოფის პროცესით ვლინდება.

**კონფიდენციალობა** - ეზრუნველყოფს მონაცემების ხელმისაწვდომობას მხოლოდ მათთვის, ვისაც ეს ინფორმაცია სჭირდება. მაგალითად, თუ თქვენ განათავსებთ ინფორმაციას ინტერნეტში, ის მედმივად იარსებებს.

**მთლიანობა** - ეზრუნველყოფს მონაცემების სიზუსტეს და სისრულეს. მაგალითისთვის, მოდიფიცირებულ/დამახინჯებულ მონაცემებს არ აქვს ღირებულება მათთვის, ვისაც ეს ინფორმაცია სჭირდება.

**ხელმისაწვდომობა** - ეზრუნველყოფს ნებისმიერ დროს ინფორმაციის ხელმისაწვდომობას ყველასთვის, ვისაც ეს ინფორმაცია სჭირდება. მაგალითად, სწრაფი და საიმედო კავშირი ხელს ეწყობს კომპიუტერული სისტემების ეფრო ეფექტიან მუშაობას.

**სენსიტიური ინფორმაცია** - ინფორმაცია, რომლის დაკარგვამ, ბოროტად გამოყენებამ, მოდიფიკაციამ ან არაავტორიზებულმა წვდომამ შეიძლება ეარყოფითად იმოქმედოს ინდივიდის კონფიდენციალურობაზე, კეთილდღეობაზე, ბიზნესის სავაჭრო საიდუმლოებაზე ან თუნდაც ეროვნულ ესაფრთხოებასა და საერთაშორისო ურთიერთობებზე.

**პერსონალური მონაცემები** - ნებისმიერი სახის ინფორმაცია, რომლითაც შესაძლებელია პირის იდენტიფიცირება. მაგალითად: თქვენი სახელი, გვარი, პირადი ნომერი, ფოტო, ვიდეო ჩანაწერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, სოციალური ქსელის ანგარიში, პირადი მიმოწერა. პერსონალური მონაცემია ასევე ინფორმაცია თქვენი სამუშაო ადგილის, შემოსავლების, ოჯახური მდგომარეობის შესახებ და სხვა.

**განსაკუთრებული კატეგორიის პერსონალური მონაცემები** - ინფორმაცია, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული კავშირის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, აღკვეთის ღონისძიების შეფარდებასთან, საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან.

**ბიომეტრიული და გენეტიკური მონაცემები** - განსაკუთრებული კატეგორიის პერსონალური მონაცემები, რომლებიც ბიომეტრიული და გენეტიკური ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა.

**Mis-information** (არასწორი ინფორმაცია) - ცრუ ინფორმაცია, რომელიც გაზიარებულია ზიანის მიყენების განზრახვის გარეშე.

**Dis-information** (დეზინფორმაცია) - ცრუ ინფორმაცია გაზიარებული განზრახ ზიანის მიყენების მიზნით.

**Mal-information** (მავნე ინფორმაცია) - სანდო ინფორმაცია, რომელიც გაზიარებულია განზრახ ზიანის მიყენების მიზნით.

**მავნე კოდი** (Malware) - განისაზღვრება, როგორც მავნე პროგრამა, რომელიც ჯაშუშურ პროგრამას (Spyware), გამომძალველ პროგრამას (Ransomware), ვირუსებსა (Virus) და ჭიებს (Worm) მოიცავს.

**გამომძალველი პროგრამა** (Ransomware) - მავნე პროგრამული უზრუნველყოფის ტიპი, რომელიც შექმნილია კომპიუტერულ სისტემაზე წვდომის დაბლოკვის მიზნით მანამ, სანამ თანხა არ გადაიხდება.

**სოციალური ინჟინერია** - მსხვერპლზე მანიპულირების, ზემოქმედების ან მოტყუების ტაქტიკა, რათა შემტევმა მოიპოვოს კონტროლი კომპიუტერულ სისტემაზე, მოიპაროს პირადი ან ფინანსური ინფორმაცია. სოციალური ინჟინერია იყენებს ფსიქოლოგიურ მანიპულაციას, რათა შემტევმა მიიღოს წვდომა სენსიტიურ ინფორმაციაზე ან აიძულოს მსხვერპლი დაარღვიოს ესაფრთხოების წესები/ნორმები.

**ფიშინგი** - სანდო სუბიექტად შენიღბვის მიზნით, ელექტრონული ფოსტის, SMS ტექსტური შეტყობინებების ან ტელეფონით სენსიტიური ინფორმაციის, მათ შორის მომხმარებლის სახელების, პაროლებისა და საკრედიტო ბარათის დეტალების მოპოვების მცდელობის პროცესს ფიშინგი ეწოდება.

**ვიშინგი** (Vishing) - სოციალური ინჟინერიის სახეობა, რომელიც ხმოვან კომუნიკაციას იყენებს.

**სმიშინგი** (Smishing) - სოციალური ინჟინერიის ფორმა, რომელიც იყენებს SMS ან ტექსტურ შეტყობინებებს.

**Denial of Service, Distributed Denial of Service** - სერვისის გათიშვა (Denial of Service) არის კიბერშეტევის ერთ-ერთი სახე, როდესაც შემტევი ბევრი მოთხოვნის წარმოქმნის გზით, ქსელს ან კომპიუტერულ სისტემას გადატვირთავს, რითიც ის ვეღარ ეპასუხებს ლეგიტიმურ მოთხოვნებს. სერვისის განაწილებული გათიშვის (Distributed Denial of Service – DDOS) შეტევაც იმავე მიზანს ემსახურება, მაგრამ ასეთ დროს შეტევას ახორციელებს არა ერთი, არამედ კომპიუტერული ქსელი (ბევრი სხვადასხვა კომპიუტერის ჩართულობით).

**Man-in-the-middle** - შეტევა ცნობილია, როგორც ჰაკერის მიერ ორ სუბიექტს შორის კომუნიკაციაში ჩარევა, რაც შემტევს (ჰაკერს) საშუალებას აძლევს წაიკითხოს და მიიღოს მხარეებს შორის გაცვლილი ინფორმაცია.

**კიბერჰიგიენა** - განმეორებითი და ზოგადი პრაქტიკა, რომელიც დაგეხმარებათ იყოთ დაცული ონლაინ სივრცეში.

**მოწყვლადობა** - სისუსტე ინფორმაციული სისტემაში, სისტემის ესაფრთხოების პროცედურებში, შიდა კონტროლში ან იმპლემენტაციაში, რომელიც შეიძლება გამოიწვიოს ან გამოიყენოს მესამე მხარემ (threat source).

**პროგრამული პატჩი** (patch) - პროგრამული ეზრუნველყოფის კომპონენტი, რომელიც ინსტალაციისას პირდაპირ ცვლის ფაილებს ან მოწყობილობის პარამეტრებს, რომლებიც დაკავშირებულია პროგრამული ეზრუნველყოფის სხვა კომპონენტთან ვერსიის ნომრის ან შესაბამისი პროგრამული კომპონენტის გამოშვების დეტალების შეცვლის გარეშე.

**მრავალფაქტორიანი ავთენტიფიკაცია** - ავთენტიფიკაციის პროცესი ორი ან მეტი ფაქტორის გამოყენებით. ფაქტორები მოიცავს: (i) ის, რაც იცით (მაგ. პაროლი/პერსონალური საიდენტიფიკაციო ნომერი (PIN)); (ii) ის, რაც გაქვთ (მაგ., კრიპტოგრაფიული იდენტიფიკაციის მოწყობილობა, ტოკენი); ან (iii) რაღაც რაც ადამიანს ეკეთვნის (მაგ., ბიომეტრიული მონაცემები).

**შიფრაცია** - მონაცემთა კრიპტოგრაფიული ტრანსფორმაცია ე.წ. „ებრალო ტექსტიდან" ე.წ. „შიფრული ტექსტში", რომელიც მალავს მონაცემთა თავდაპირველ მნიშვნელობას, რათა თავიდან აიცილოს მისი გამჟღავნება ან გამოყენება. თე ტრანსფორმაცია შექცევადია, შესაბამის შებრუნების პროცესს ეწოდება "დეშიფრაცია", რომელიც არის ტრანსფორმაცია, რომელიც აღადგენს დაშიფრულ მონაცემებს თავდაპირველ მდგომარეობაში.

**სარეზერვო ასლები** - საჭიროების შემთხვევაში აღდგენის გასაადვილებლად შექმნილი ფაილებისა და პროგრამების ასლი.

**როუტერი** - საკომენიკაციო მოწყობილობა, რომელიც გადასცემს შეტყობინებებს ორ ქსელს შორის.

# 1. კიბერუსაფრთხოების ზოგადი პრინციპები

## 1.1. რა არის კიბერუსაფრთხოება?

კიბერუსაფრთხოება წარმოადგენს ქსელების, მოწყობილობებისა და მონაცემების დაცვას უკანონო ქმედებისგან, წვდომისგან ან კრიმინალური გამოყენებისგან, რომელიც ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფის პროცესით ვლინდება. თქვენი პირადი ინფორმაციის დიდი ნაწილი ინახება თქვენს კომპიუტერში, სმარტფონსა ან პლანშეტში. იმის ცოდნა, თუ როგორ დაიცვათ თქვენი ინფორმაცია, მნიშვნელოვანია, არა მხოლოდ ინდივიდებისთვის, არამედ ორგანიზაციებისთვისაც. ყოველ ჯერზე, როცა ინტერნეტს იყენებთ, თქვენ დგახართ უსაფრთხოებასთან დაკავშირებული არჩევანის წინაშე. თქვენი და სახელმწიფოს უსაფრთხოება დამოკიდებულია ონლაინ სივრცეში პასუხისმგებლიან გადაწყვეტილებებზე. უსაფრთხო ინტერნეტისთვის, აუცილებელია, ყველა ჩვენგანმა გააცნობიეროს საკუთარი კიბერპასუხისმგებლობა.


როგორც განმარტებაში აღინიშნა, კიბერუსაფრთხოების მიზანია, უზრუნველყოფილი იქნეს ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა.

- **კონფიდენციალობა** - უზრუნველყოფს მონაცემების ხელმისაწვდომობას მხოლოდ მათთვის, ვისაც ეს ინფორმა-

ცია სჭირდება. მაგალითად, თუ თქვენ განათავსებთ ინფორმაციას ინტერნეტში, ის მუდმივად იარსებებს.

- **მთლიანობა -** უზრუნველყოფს მონაცემების სიზუსტეს და სისრულეს. მაგალითისთვის, მოდიფიცირებულ/დამახინჯებულ მონაცემებს არ აქვს ღირებულება მათთვის, ვისაც ეს ინფორმაცია სჭირდება.
- **ხელმისაწვდომობა -** უზრუნველყოფს ნებისმიერ დროს ინფორმაციის ხელმისაწვდომობას ყველასთვის, ვისაც ეს ინფორმაცია სჭირდება. მაგალითად, სწრაფი და საიმედო კავშირი ხელს უწყობს კომპიუტერული სისტემების უფრო ეფექტიან მუშაობას.

## 1.2. საფრთხეები

### 1.2.1. მავნე კოდი

მავნე კოდი (Malware) განისაზღვრება, როგორც მავნე პროგრამა, რომელიც ჯაშუშურ პროგრამას (spyware), გამომძალველ პროგრამას (ransomware), ვირუსებსა (Virus) და ჭიებს (Worm) მოიცავს. მავნე პროგრამა შეიძლება ამოქმედდეს მაშინ, როდესაც მომხმარებელი დააწკაპებს ელექტრონული ფოსტის მავნე დანართზე ან ბმულზე, რაც იწვევს მავნე პროგრამული უზრუნველყოფის ინსტალაციას მომხმარებლის კომპიუტერულ სისტემაში. ზოგიერთ მავნე პროგრამას შეუძლია:

- კომპიუტერული ქსელის კრიტიკულ კომპონენტებზე წვდომა გამოსასყიდის მიღების მიზნით (ransomware) შეზღუდოს.
- დააინსტალიროს ახალი, დამატებითი მავნე პროგრამული უზრუნველყოფა.
- ფარულად მოიპოვოს ინფორმაცია მყარი დისკიდან (ჯაშუშური პროგრამა - spyware).

- გაანადგუროს და გამოუყენებელი გახადოს კომპიუტერული სისტემის ცალკეული კომპონენტები.

### 1.2.2. პიროვნების მიტაცება და თაღლითობები

პიროვნების მიტაცება (identity theft) და თაღლითობები დანაშაულია, რომლის მსხვერპლი შეიძლება გახდეს ისიც კი, ვინც კომპიუტერს არასდროს იყენებს. არსებობს მრავალი გზა, როდესაც კრიმინალებს შეუძლიათ წვდომა მოიპოვონ თქვენს ინფორმაციაზე, მოიპარონ თქვენი ელექტრონული საფულე, მოისმინონ თქვენი სატელეფონო ზარი, აიღონ გადაგდებული დოკუმენტი, რომელიც თქვენი ანგარიშის ნომერს შეიცავს.

### 1.2.3. Denial of Service

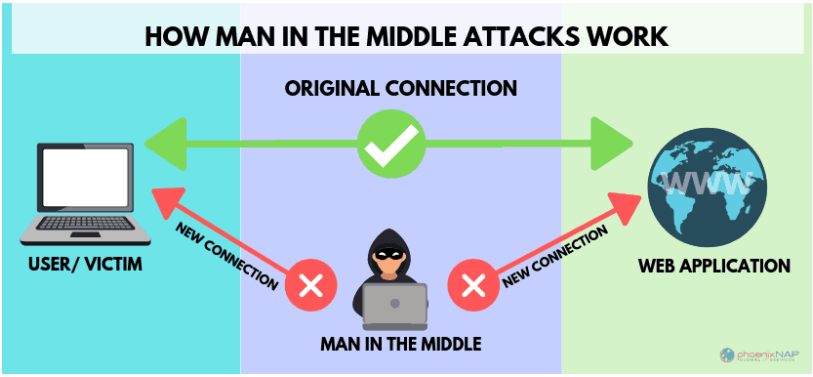
სერვისის გათიშვა (Denial of Service) არის კიბერშეტევის ერთ-ერთი სახე, როდესაც შემტევი ბევრი მოთხოვნის წარმოქმნის გზით, ქსელს ან კომპიუტერულ სისტემას გადატვირთავს, რითიც ის ვეღარ უპასუხებს ლეგიტიმურ მოთხოვნებს. სერვისის განაწილებული გათიშვის (Distributed Denial of Service – DDOS) შეტევაც იმავე მიზანს ემსახურება, მაგრამ ასეთ დროს შეტევას ახორციელებს არა ერთი, არამედ კომპიუტერული ქსელი (ბევრი სხვადასხვა კომპიუტერის ჩართულობით). მსგავსი შეტევები შესაძლოა დამატებით სხვა მიზანს ემსახურებოდეს - კიბერ-შემტევს შეუძლია ეფექტურად გამოიყენოს დრო მანამ, სანამ ქსელი გაუმართავია და დაიწყოს შემდგომი თავდასხმები.

ამასთან, საყურადღებოა, რომ არსებობს ბოტნეტი (botnet), რომელიც არის ერთგვარი DDoS შეტევის სახეს წარმოადგენს. ასეთ დროს, შემტევები (ჰაკერები) შეიძლება იყენებდნენ მილიონობით გატეხილ (კომპრომიტირებულ) მოწყობილობას. ბოტნეტებს ხშირად ზომბი სისტემებადაც მოიხსენიებენ, რომლებიც თავს ესხმიან სამიზნე სისტემებს და ცდილობენ გადატვირთონ მათი შესაძლებლობები. ბოტნეტი შეიძლება

განლაგებული იყოს მსოფლიოს სხვადასხვა კუთხეში, რაც ართულებს მისთვის თვალყურის დევნებას.

### 1.2.4. Man in the Middle

Man-in-the-middle შეტევა ცნობილია, როგორც ჰაკერის მიერ ორ სუბიექტს შორის კომუნიკაციაში ჩარევა, რაც შემტევს (ჰაკერს) საშუალებას აძლევს წაიკითხოს და მიიღოს მხარეებს შორის გაცვლილი ინფორმაცია. MITM შეტევები ხშირია, როდესაც ვიზიტორები უკავშირდებიან დაუცველ (დაუშიფრავ) საჯარო Wi-Fi ქსელს.




### 1.2.5. Phishing

სანდო სუბიექტად შენიღბვის მიზნით, ელექტრონული ფოსტის, SMS ტექსტური შეტყობინებების ან ტელეფონით სენსიტიური ინფორმაციის, მათ შორის მომხმარებლის სახელების, პაროლებისა და საკრედიტო ბარათის დეტალების მოპოვების მცდელობის პროცესს ფიშინგი ეწოდება. ფიშინგ შეტევისას, შემტევი ქმნის გადაუდებლობის, ცნობისმოყვარეობის ან შიშის გრძნობას. ფიშინგ შეტყობინება მსხვერპლს უბიძგებს გასცეს სენსიტიური ინფორმაცია, დააწკაპოს მავნე ვებსაიტების ბმულებზე ან გახსნას დანართები, რომლებიც მავნე პროგრამას შეიცავს.

### 1.2.6. პაროლის გატეხვა (Password Cracking)

კიბერ თავდამსხმელს შეუძლია ადვილად მიიღოს წვდომა უამრავ ინფორმაციაზე თუ ხელში ჩაიგდებს მომხმარებლის პაროლს. არსებობს პაროლის გატეხვის სხვადასხვა გზა:

- გადარჩევა (brute force attack) - ჰაკერი უბრალოდ გამოიცნობს მომხმარებლის პაროლს შესაბამისი მინიშნებების საფუძველზე (მაგალითად, დაბადების დღე, ძაღლის სახელი და ა.შ), თუმცა გადარჩევის შეტევა შეიძლება იყოს უფრო დახვეწილი და რთულიც. მაგალითად, ბევრი ადამიანი იყენებს ერთსადაიმავე პაროლს სხვადასხვა სისტემისთვის. ზოგიერთი პაროლი შეიძლება ხელმისაწვდომი იყოს ონლაინ, გატეხილი (გაჟონილი) საიტების ბაზებში და, შესაბამისად, ჰაკერმა შეიძლება გამოიყენოს თქვენი გაჟონილი პაროლი სხვა სისტემების გასატეხად.
- ლექსიკონის შეტევა (Dictionary attack) - ლექსიკონის შეტევა გადარჩევის შეტევის (brute force attack) ოდნავ უფრო დახვეწილი მაგალითია. ის იყენებს ავტომატიზებულ პროცესს, როდესაც შემტევი ცდილობს გამოიცნოს თქვენი პაროლი ხშირად გამოყენებული პაროლებისა და ფრაზების სიის საფუძველზე (მაგალითად, ბევრი მომხმარებელი იყენებს შემდეგ პაროლებს: 123456, qwerty, password, etc.). ლექსიკონების უმეტესობა ყველაზე გავრცელებული პაროლებისა და სიტყვების კომბინაციებისგან შედგება. ადამიანები ხშირად დასამახსოვრებელ ფრაზებს იყენებენ პაროლებად, რომლებიც, როგორც წესი, სიტყვების სახით არის წარმოდგენილი. ეს არის დიდწილად მიზეზი იმისა, რის გამოც სისტემები ადამიანებს მრავალსიმბოლოიანი ტიპის პაროლების გამოყენებისკენ მოუწოდებენ.

## 1.3. დაცვის მექანიზმები - კიბერჰიგიენა

### 1.3.1. აქციეთ კიბერჰიგიენა თქვენი რუტინის ნაწილად

თქვენი კიბერუსაფრთხოების რეგულარული მონიტორინგი კიბერსაფრთხეების რეალიზების რისკებს ამცირებს. ისევე, როგორც ნებისმიერი ჩვევა, კიბერჰიგიენაც რუტინას და განმეორებითობას მოითხოვს.

კიბერჰიგიენის პროცესი დაიწყეთ ე.წ. „შეხსენების“ (Reminder) დაყენებით ან კალენდრში თარიღების მონიშვნით, რათა თქვენს მოწყობილობასთან დაკავშირებული მთელი რიგი ამოცანები გადაწყვიტოთ - ვირუსების სკანირება ანტივირუსული პროგრამული უზრუნველყოფით, ყველა თქვენი მოწყობილობის ოპერაციული სისტემის განახლება, უსაფრთხოების პატჩების შემოწმება, მყარი დისკის წაშლა და თქვენი პაროლების შეცვლა.

### 1.3.2. ძირითადი ნაბიჯები კიბერჰიგიენისთვის

კიბერჰიგიენა არის ზოგადი პრაქტიკა, რომელიც დაგეხმარებათ იყოთ დაცული ონლაინ სივრცეში. წინამდებარე დოკუმენტში განხილულია კიბერჰიგიენის უკეთესი პრაქტიკის მაგალითი, რომელიც ცხრა აუცილებელ ნაბიჯს მოიცავს.

ნაბიჯი 1: დააინსტალირეთ სანდო ანტივირუსული პროგრამული უზრუნველყოფა

პირველი და შესაძლოა ყველაზე მნიშვნელოვანი ნაბიჯი არის ანტივირუსული პროგრამის დაყენება. რისთვის არის შექმნილი? ანტივირუსული პროგრამა არის პროგრამა ან პროგრამების ერთობა, რომელიც ასკანერებს და პოულობს კომპიუტერულ ვირუსებს ან სხვა მავნე პროგრამებს. კერძოდ, ანტივირუსული პროგრამა უზრუნველყოფს:

- იპოვოს ის ფაილები, რომლებიც მავნე კოდს (პროგრამას) შეიცავს.
- ავტომატური სკანირების დაგეგმვასა და შესრულებას.
- ერთი კონკრეტული ფაილის, მთელი თქვენი კომპიუტერის, ან ფლეშ დრაივის სკანირებას თქვენი კონკრეტული საჭიროებიდან გამომდინარე.
- მავნე კოდებისა და პროგრამული უზრუნველყოფების წაშლას.

ნაბიჯი 2: გამოიყენეთ ქსელის „ფაერვოლი“

ქსელის firewall-ის გამოყენება კიდევ ერთი მთავარი ნაბიჯია კიბერჰიგიენის შესანარჩუნებლად. Firewalls არის დაცვის პირველი ხაზი ქსელის უსაფრთხოებაში, რაც ხელს უშლის არაავტორიზებული მომხმარებლების წვდომას თქვენს ვებსაიტებზე, ელფოსტის სერვერებსა და ინფორმაციის სხვა წყაროებზე, რომლებზე წვდომაც ინტერნეტიდანაა შესაძლებელი.

ნაბიჯი 3: რეგულარულად განაახლეთ პროგრამული უზრუნველყოფა

რეგულარულად განაახლეთ თქვენი აპლიკაციები, ვებ ბრაუზერები და ოპერაციული სისტემები, რათა დარწმუნდეთ, რომ ისეთ უახლეს პროგრამებთან მუშაობთ, რომლებშიც

აღმოფხვრილია ან გასწორებულია უსაფრთხოების ხარვეზები (მოწყვლადობა). ეს განახლებები განსაკუთრებით მნიშვნელოვანია, რადგან ისინი ხშირად შეიცავს პროგრამული უზრუნველყოფის პატჩებს (patch). პროგრამული უზრუნველყოფის დეველოპერები (აპლიკაციის მწარმოებელი კომპანიები) უშვებენ/აქვეყნებენ უსაფრთხოების პატჩებს, როდესაც აღმოაჩენენ პროგრამული უზრუნველყოფის ხარვეზებს, რომლებსაც შემტევი

ჰაკერები სისტემებში შესაღწევად იყენებენ.

ნაბიჯი 4: დააყენეთ ძლიერი პაროლები

ძლიერი პაროლების დაყენება თქვენი ყველა მოწყობილობისთვის აუცილებელია. თქვენი პაროლი უნდა იყოს უნიკალური და რთული, შეიცავდეს მინიმუმ 12 სიმბოლოს ციფრებთან, სიმბოლოებთან და როგორც დიდ, ასევე პატარა ასოებთან ერთად. თქვენი პაროლის რეგულარულად შეცვლა (და არა გაზიარება ან ხელახლა გამოყენება) გიცავთ ჰაკერებისგან.

ნაბიჯი 5: გამოიყენეთ მრავალფაქტორიანი ავთენტიფიკაცია

ორფაქტორიანი ან მრავალფაქტორიანი ავთენტიფიკაცია არის საუკეთესო პრაქტიკა, რომელიც გთავაზობთ დაცვის დამატებით საშუალებას. ორფაქტორიანი ავთენტიფიკაცია, როგორც წესი, მოითხოვს თქვენი პაროლისა და მომხმარებლის სახელის წარდგენას უნიკალურ კოდთან ერთად, რომელიც მობილურ ტელეფონში იგზავნება. მრავალფაქტორიანი ავთენტიფიკაცია, ბიომეტრიის გამოყენებით, უსაფრთხოების დამატებით ფენებს ამატებს, როგორიცაა სახის ან თითის ანაბეჭდის ამოცნობა, რათა ჰაკერებისთვის თქვენს მოწყობილობასა და პირად ინფორმაციაზე წვდომა გაართულოს.

ნაბიჯი 6: გამოიყენეთ მოწყობილობის დაშიფვრა

მიუხედავად იმისა, რომ კომპანიების უმეტესობას ავტომატურად აქვს მონაცემთა დაშიფვრის ფუნქცია, ასევე შეიძლება დაგჭირდეთ თქვენი მოწყობილობების და სხვა მედია მატარებლების (მაგალითად, USB flash drive) დაშიფვრა, რომლებიც შეიცავს სენსიტიურ მონაცემებს - მათ შორის ლეპტოპებს, ტაბლეტებს, სმარტფონებს, დისკებს, სარეზერვო ფაილებსა და ღრუბლოვან (cloud) საცავს. ხშირად, ბევრი მოწყობილობა დაშიფვრას იყენებს, როგორც ნაგულისხმევ ფუნქციას სმარტფონებზე შენახული მონაცემებისთვის.

ზოგიერთი აპლიკაცია სრულ შიფრაციას იყენებს, ხოლო სხვა სერვისები შიფრავს თქვენს მოწყობილობებზე არსებულ მონაცემებს და ქმნის მათ სარეზერვო ასლებს ქლაუდში. დამატებით, კიდევ ერთი ვარიანტია დაშიფრული USB მეხსიერების დისკის გამოყენება სენსიტიური მონაცემების დასაცავად.

ნაბიჯი 7: რეგულარულად შექმენით სარეზერვო ასლები

მნიშვნელოვანია, რომ შექმნათ თქვენთვის ღირებული ფაილების სარეზერვო ასლები ოფლაინ, გარე მყარ დისკზე ან ქლაუდში. აღნიშნული დაგეხმარებათ დაიცვათ თქვენთვის მნიშვნელოვანი ფაილები სხვადასხვა ტიპის მონაცემთა დაკარგვის რისკებისგან, განსაკუთრებით მაშინ, თუ ჰაკერები წვდომას თქვენს ერთ-ერთ მოწყობილობაზე მიიღებენ.

ნაბიჯი 8: გაასუფთავეთ მყარი დისკი

თუ თქვენ საკუთარ ლეპტოპს, ტაბლეტს ან სმარტფონს ყიდით, მნიშვნელოვანია უზრუნველყოთ უსაფრთხოების ზომები, რათა მყიდველს ხელში არ ჩაუვარდეს თქვენ შესახებ პერსონალური ან სენსიტიური ინფორმაცია. თუ თქვენს მოწყობილობას გატეხავენ, სუფთა მყარი დისკი ნიშნავს ნაკლებ ინფორმაციას, რომელზე წვდომაც შემტევებს ექნებათ. თუმცა, მხოლოდ ფაილების ან მონაცემების წაშლა შეიძლება არ იყოს საკმარისი. კარგი კიბერჰიგიენისთვის, აუცილებელია დისკის დაფორმატება და შემდეგ დისკის გაწმენდა (wipe out). მაგალითად, თუ გსურთ გაყიდოთ თქვენი კომპიუტერი, რომელსაც ონლაინ ბანკინგისთვის იყენებდით, უნდა იფიქროთ დისკის გასუფთავებაზე, რათა თქვენი მყარი დისკიდან პროგრამული უზრუნველყოფა და მონაცემები წაიშალოს.

ნაბიჯი 9: დაიცავით თქვენი როუტერი

არ დაგავიწყდეთ თქვენი უკაბელო ქსელის დაცვა. ამისათვის, აუცილებელია, შეცვალოთ ნაგულისხმევი სახელი და პაროლი,

რომელიც როუტერს მწარმოებლისგან მოჰყვა. ასევე, აუცილებელია, გამორთოთ დისტანციური მართვის ფუნქცია მისი დაყენების შემდეგ. დამატებით, დარწმუნდით, რომ თქვენი როუტერი გთავაზობთ WPA2 ან WPA3 დაშიფვრას ქსელის მეშვეობით გაგზავნილი ინფორმაციის კონფიდენციალურობის უმაღლესი დონის შესანარჩუნებლად.

## 1.4. კიბერუსაფრთხოება პატარა და საშუალო ორგანიზაციებისთვის

წინამდებარე სახელმძღვანელოში მოცემული ხუთი სწრაფი და მარტივი ნაბიჯი, რომელიც დაგეხმარებათ, დაზოგოთ დრო, ფული და დაიცვათ თქვენი ორგანიზაციის რეპუტაცია. სახელმძღვანელო არ იძლევა გარანტიას ყველა სახის კიბერშეტევისგან თავის დასაცავად, თუმცა ქვემოთ მოყვანილი ნაბიჯები მნიშვნელოვნად შეამცირებს საფრთხის შანსს, რათა თქვენი ბიზნესი/ორგანიზაცია კიბერდანაშაულის მსხვერპლი არ გახდეს.

### 1.4.1. ნაბიჯი 1 - თქვენი მონაცემების სარეზერვო ასლის შექმნა

იფიქრეთ იმაზე, თუ რამდენად დამოკიდებულია თქვენი ორგანიზაცია ისეთ მნიშვნელოვან მონაცემებზე, როგორიცაა მომხმარებლის/მოქალაქეების ინფორმაცია, შეთავაზებები, შეკვეთები და გადახდის დეტალები. ახლა წარმოიდგინეთ, რამდენ ხანს შეძლებთ მათ გარეშე მუშაობას.

ყველა ბიზნესმა თუ ორგანიზაციამ, განურჩევლად სიდიდისა, რეგულარულად უნდა მოამზადოს მნიშვნელოვანი ინფორმაციის სარეზერვო ასლები და უნდა დარწმუნდეს, რომ ეს სარეზერვო ასლები ბოლოა (up-to-date) და მათი აღდგენა საჭიროების შემთხვევაში შესაძლებელია. ამით დარწმუნდებით, რომ თქვენი ორგანიზაცია შეძლებს გააგრძელოს ფუნქციონირება წყალდიდო-

ბის, ხანძრის, ფიზიკური დაზიანების ან ქურდობის მოვლენების შემდეგაც კი. გარდა ამისა, თუ თქვენ გაქვთ მონაცემების სარეზერვო ასლები, რომელთა აღდგენაც სწრაფად შეგიძლიათ, მაშინ თქვენი ორგანიზაცია ნაკლებად მოწყვლადია გამოსასყიდის შეტევების მიმართ (ransomware attacks).

წინამდებარე თავებში მოცემულია ხუთი რჩევა, რომელიც უნდა გაითვალისწინოთ თქვენი მონაცემების სარეზერვო ასლის შექმნისას.

### რჩევა 1: განსაზღვრეთ რა მონაცემების სარეზერვო ასლი გჭირდებათ

პირველი ნაბიჯი არის თქვენთვის კრიტიკული მონაცემების იდენტიფიცირება. ანუ, ინფორმაცია, რომლის გარეშეც თქვენი ბიზნესი ვერ იმუშავებს. ჩვეულებრივ, ეს მოიცავს დოკუმენტებს, ფოტოებს, ელექტრონულ ფოსტას, კონტაქტებსა და კალენდრებს, რომელთა უმეტესობა თქვენი კომპიუტერის, ტელეფონის, ტაბლეტის ან ქსელის რამდენიმე ჩვეულებრივ საქაღალდეში ინახება.

### რჩევა 2: შეინახეთ სარეზერვო ასლი კომპიუტერისგან განცალკევებით

იქნება ეს USB მატარებელზე, ცალკეულ დისკზე თუ ცალკე კომპიუტერზე, მონაცემთა სარეზერვო ასლების წვდომა უნდა შეიზღუდოს ისე, რომ ისინი:

- არ არის ხელმისაწვდომი პერსონალისთვის;
- არ არიან მუდმივად დაკავშირებული (ფიზიკურად ან ლოკალურ ქსელში) მოწყობილობასთან, რომელსაც აქვს ორიგინალი ასლი;
- Ransomware (და სხვა მავნე პროგრამა) ხშირად შეიძლება ავტომატურად გადავიდეს მიმაგრებულ საცავში, რაც ნიშნავს

იმას, რომ ნებისმიერი ასეთი სარეზერვო ასლი ასევე შეიძლება დაინფიცირდეს და არ დარჩეს აღსადგენი სარეზერვო ასლი. მეტი მედეგობისთვის, თქვენ უნდა იფიქროთ საკუთარი სარეზერვო ასლების სხვა ადგილას შენახვაზე. ასე ხანძარი ან ქურდობა არ გამოიწვევს ორივე ასლის დაკარგვას. ამის მისაღწევად, ღრუბლოვანი შენახვის გადაწყვეტილებები (იხ. ქვემოთ) არის ეკონომიური და ეფექტური გზა.

რჩევა 3: განიხილეთ ღრუბლოვანი საცავი

თქვენ ალბათ უკვე იყენებთ ღრუბლოვან (ე.წ.ქლაუდ) საცავს თქვენს ყოველდღიურ სამუშაოსა და პირად ცხოვრებაში ისე, რომ არც კი იცით ამის შესახებ. როგორც წესი, თუ თქვენ არ გაქვთ საკუთარი ელექტრონული ფოსტის სერვერი, თქვენი ელ. ფოსტა უკვე ინახება „ღრუბელში“.

ღრუბლოვანი საცავის გამოყენება (სადაც სერვისის პროვაიდერი თავის ინფრასტრუქტურაში თქვენს მონაცემებს ინახავს) გულისხმობს იმას, რომ თქვენი მონაცემები ფიზიკურად განცალკევებულია თქვენი მდებარეობიდან. ასეთ შემთხვევაში, თქვენ ასევე ისარგებლებთ ხელმისაწვდომობის მაღალი ხარისხით. სერვისის პროვაიდერებს შეუძლიათ მიაწოდონ თქვენს ორგანიზაციას მონაცემები და ვებ-სერვისები ისე, რომ არ დაგჭირდეთ ძვირადღირებულ აპარატურაში წინასწარ ინვესტირება. პროვაიდერების უმეტესობა გვთავაზობს შესანახი სივრცის შეზღუდულ ოდენობას უფასოდ (მაგალითად, Google Drive გვთავაზობს 15 GB-მდე სანახს უფასოდ) და უფრო დიდი საცავის ტევადობას მინიმალური დანახარჯებით მცირე ბიზნესისთვის.

რჩევა 4: წაიკითხეთ ღრუბლოვანი უსაფრთხოების ინსტრუქცია

ყველა სერვისის პროვაიდერი ერთნაირი არ არის, მაგრამ ბაზარი საკმაოდ მომწიფებულია და პროვაიდერთა უმეტესობას აქვს ჩაშენებული უსაფრთხოების კარგი პრაქტიკა. თქვენი IT სერვისების მნიშვნელოვანი ნაწილების სერვისის პროვაიდერისთვის გადაცემით, თქვენ ისარგებლებთ სპეციალიზებული გამოცდილებით, რომელიც ხშირად არ არის ხელმისაწვდომი მცირე და საშუალო ზომის ორგანიზაციებისთვის. თუმცა, სანამ სერვის პროვაიდერებს დაუკავშირდებით, გირჩევთ გაეცნოთ ღრუბლოვანი უსაფრთხოების საერთაშორისო პრაქტიკას.

რჩევა 5: სარეზერვო ასლის შექმნა თქვენი ყოველდღიური ბიზნესის ნაწილად აქციეთ

ორგანიზაციებისთვის, სარეზერვო ასლის შექმნა არც ისე საინტერესო პროცესია (და ყოველთვის იქნება უფრო მნიშვნელოვანი ამოცანები, რომლებიც, თქვენი აზრით, პრიორიტეტული უნდა იყოს), მაგრამ ქსელის ან ღრუბლოვანი საცავის გადაწყვეტილებების უმრავლესობა, ახლა საშუალებას გაძლევთ, ავტომატურად გააკეთოთ სარეზერვო ასლები. მაგალითად, როდესაც გარკვეული ტიპის ახალი ფაილები მითითებულ საქაღალდეებში ინახება. ავტომატური სარეზერვო ასლების გამოყენება არა მხოლოდ დაგიზოგავთ დროს, არამედ უზრუნველყოფს თქვენი ფაილების უახლესი ვერსიის არსებობას იმ შემთხვევაში, თუ ისინი დაგჭირდებათ.

ბევრი სარეზერვო გადაწყვეტა (back-up solution) მარტივია და ხელმისაწვდომია ბიზნესისთვის კრიტიკული უსაფრთხოების კონტროლების გათვალისწინებით. გადაწყვეტის (პროგრამული უზრუნველყოფის) არჩევისას, ასევე უნდა გაითვალისწინოთ, რა რაოდენობის მონაცემი გჭირდებათ სარეზერვო ასლის შესაქმნელად და რამდენად სწრაფად უნდა შეძლოთ მონაცემებზე წვდო-

მა ნებისმიერი ინციდენტის შემდეგ.

### 1.4.2. ნაბიჯი 2 - თქვენი ორგანიზაციის დაცვა მავნე პროგრამებისგან

მავნე პროგრამული უზრუნველყოფა (ასევე ცნობილი, როგორც „მავნე პროგრამა“) არის პროგრამული უზრუნველყოფა ან ვებ კონტენტი, რომელსაც შეუძლია ზიანი მიაყენოს თქვენს ორგანიზაციას. მავნე პროგრამის ყველაზე ცნობილი ფორმაა ვირუსები, თვითკოპირებული პროგრამები, რომლებიც აინფიცირებენ ლეგიტიმურ პროგრამულ უზრუნველყოფას.

წინამდებარე თავები შეიცავს ხუთ უფასო და ადვილად განსახორციელებელ რჩევას, რომლებიც დაგეხმარებათ თავიდან აიცილოთ მავნე პროგრამები თქვენი ორგანიზაციის დაზიანებისგან.

რჩევა 1: დააინსტალირეთ ან/და ჩართეთ ანტივირუსული პროგრამა

ანტივირუსული პროგრამა - რომელიც ხშირად უფასოდ შედის პოპულარულ ოპერაციულ სისტემებში - უნდა იყოს გამოყენებული ყველა კომპიუტერსა და ლეპტოპში. თქვენი საოფისე აღჭურვილობისთვის შეგიძლიათ დააწკაპოთ "ჩართვას", რითიც გააქტიურებთ პროგრამას.

რჩევა 2: შეუზღუდეთ პერსონალს აკრძალული აპლიკაციების ჩამოტვირთვა

თქვენ უნდა ჩამოტვირთოთ აპლიკაციები მობილური ტელეფონებისთვის და ტაბლეტებისთვის მხოლოდ მწარმოებლის მიერ დამტკიცებული ე.წ. „მარკეტფლეისებიდან“ (როგორიცაა Google Play ან Apple App Store). აქ არსებული აპლიკაციები შემოწმებულია, რათა უზრუნველყონ გარკვეული დონის დაცვა მავნე პროგრამებისგან. თქვენ უნდა შეზღუდოთ

პერსონალის მიერ არასანდო (მესამე მხარის) აპლიკაციების ჩამოტვირთა უცნობი მომწოდებლებისგან.

ორგანიზაციის პერსონალის ანგარიშებს უნდა ჰქონდეს საკმარისი წვდომა, რომელიც საჭიროა მათი როლის შესასრულებლად, ხოლო დამატებითი ნებართვები (მაგ. ადმინისტრატორის უფლებები) უნდა იყოს მხოლოდ მათთვის, ვისაც ეს სჭირდება. როდესაც ადმინისტრაციული ანგარიშები (accounts) იქმნება, ისინი უნდა იქნეს გამოყენებული მხოლოდ ამ კონკრეტული ამოცანისთვის (ადმინისტრირებისთვის), ხოლო სტანდარტული მომხმარებლის ანგარიშები ზოგადი სამუშაოსთვის უნდა გამოიყენებოდეს.

რჩევა 3: განაახლეთ მთელი თქვენი IT ინფრასტრუქტურა (პატჩინგი)

დარწმუნდით, რომ პროგრამული უზრუნველყოფა არის განახლებული თქვენი IT ინფრასტრუქტურისთვის (მაგ. ტაბლეტები, სმარტფონები, ლეპტოპები და კომპიუტერები) შემქმნელების, აპარატურის მომწოდებლებისა და გამყიდველების უახლესი ვერსიებით. ამ განახლებების გამოყენება (პროცესი, რომელიც ცნობილია როგორც პაჩინგი) არის ერთ-ერთი ყველაზე მნიშვნელოვანი რამ, რისი გაკეთებაც შეგიძლიათ უსაფრთხოების გასაუმჯობესებლად. ოპერაციული სისტემები, პროგრამები, ტელეფონები და აპლიკაციები უნდა იყოს დაყენებული „ავტომატურ განახლებაზე“.

საყურადღებოა, რომ რაღაც მომენტში, განახლებები აღარ იქნება ხელმისაწვდომი (რადგან ყველა პროდუქტს აქვს მხარდაჭერის სერვისის საციცოცხლო ციკლი), რა დროსაც თქვენ უნდა განიხილოთ მისი შეცვლა თანამედროვე ალტერნატივით.

რჩევა 4: აკონტროლეთ USB დისკების და მეხსიერების ბარათების გამოყენება

ყველამ ვიცით, რამდენად მაცდურია USB დისკების ან მეხსიერების ბარათების გამოყენება ორგანიზაციებსა და ადამიანებს შორის ფაილების გადასატანად. თუმცა ერთი მომხმარებლის მიერ ინფიცირებული USB ფლეშ მეხსიერების ბარათის გამოყენებაც კი საკმარისია, რომ განადგურდეს მთელი ორგანიზაციის ინფორმაცია.

როდესაც დისკები და ფლეშ მეხსიერების ბარათები ღიად არის გაზიარებული, ძნელია თვალყური ადევნოთ, რას შეიცავს ან ვინ გამოიყენა ისინი. თქვენ შეგიძლიათ შეამციროთ ინფიცირების (დავირუსების) ალბათობა შემდეგი გზით:

- ფიზიკურ პორტებზე წვდომის დაბლოკვით მომხმარებლების უმეტესობისთვის;
- ანტივირუსული საშუალებების გამოყენებით;
- მხოლოდ დამტკიცებული დისკების და ბარათების გამოყენების უფლებით თქვენს ორგანიზაციაში - და არსად სხვაგან.

აქციეთ ეს დირექტივები თქვენი ორგანიზაციის/კომპანიის პოლიტიკის ნაწილად, რათა შეძლოთ თქვენი ორგანიზაციისთვის არასასურველი რისკების თავიდან აცილება. ასევე, შეგიძლიათ სთხოვოთ პერსონალს ფაილების გადატანა ალტერნატიული საშუალებების გამოყენებით (როგორიცაა ელექტრონული ფოსტით ან ღრუბლოვანი სერვისებით) და არა USB ფლეშ მეხსიერების ბარათით.

რჩევა 5: ჩართეთ თქვენი firewall

Firewall-ები ქმნიან „ბუფერულ ზონას“ თქვენს საკუთარ ქსელსა და გარე ქსელებს შორის (როგორიცაა ინტერნეტი). ყველაზე პოპულარულ ოპერაციულ სისტემებში ახლა უკვე შედის firewall.

### 1.4.3. ნაბიჯი 3 - თქვენი სმარტფონების და ტაბლეტების უსაფრთხოების დაცვა

მობილური ტექნოლოგია ახლა თანამედროვე ორგანიზაციის/ბიზნესის არსებითი ნაწილია. ჩვენი მონაცემების დიდი ნაწილი ინახება ტაბლეტებზე და სმარტფონებზე. უფრო მეტიც, ეს

მოწყობილობები ახლა ისეთივე ძლიერია, როგორც ტრადიციული კომპიუტერები და იმის გამო, რომ ისინი ხშირად ტოვებენ ოფისის და სახლის უსაფრთხოებას, მათ უფრო მეტი დაცვა სჭირდებათ, ვიდრე "დესკტოპ" აღჭურვილობას.

ამის გათვალისწინებით, წინამდებარე თავებში, მოცემულია 5 რჩევა, რომელიც თქვენი მობილური მოწყობილობებისა და მათზე შენახული ინფორმაციის უსაფრთხოების შენარჩუნებაში დაგეხმარებათ.

რჩევა 1: ჩართეთ პაროლით დაცვა

სათანადოდ რთული PIN ან პაროლი (და არა ისეთი, რომლის გამოცნობა ან ამოცნობა შესაძლებელია თქვენი სოციალური მედიის პროფილებიდან) ხელს შეუშლის საშუალო დონის კრიმინალს თქვენს ტელეფონზე წვდომის მოპოვებაში. დღეს ბევრ მოწყობილობას აქვს თითის ანაბეჭდის ამოცნობა თქვენი მოწყობილობის დასაბლოკად, პაროლის საჭიროების გარეშე. თუმცა ეს ფუნქციები ყოველთვის არ არის გააქტიურებული, ამიტომ შეამოწმეთ - გაქვთ თუ არა ჩართული.

რჩევა 2: დარწმუნდით, რომ დაკარგული ან მოპარული მოწყობილობების თვალყურის დევნება, დაბლოკვა ან წაშლა შესაძლებელია

თანამშრომლების ტაბლეტები ან ტელეფონები შეიძლება დაიკარგოს ან ვიღაცამ მოიპაროს. საბედნიეროდ, მოწყობილობე-

ბის უმეტესობას აქვს უფასო ვებ ინსტრუმენტები, რომლებიც ფასდაუდებელია თქვენი მოწყობილობის დაკარგვის შემთხვევაში. თქვენ შეგიძლიათ გამოიყენოთ ისინი, რათა:

- აკონტროლოთ მოწყობილობის მდებარეობა;
- მოწყობილობაზე წვდომა დისტანციურად ჩაკეტოთ;
- დისტანციურად წაშალოთ მოწყობილობაზე შენახული მონაცემები;
- მიიღოთ მოწყობილობაში შენახული მონაცემების სარეზერვო ასლი.

ამ ხელსაწყოების დაყენება თქვენი ორგანიზაციის ყველა მოწყობილობაზე თავიდან შეიძლება რთულად მოგეჩვენოთ, მაგრამ მობილური მოწყობილობების მართვის პროგრამული უზრუნველყოფის გამოყენებით, შეგიძლიათ ერთი დაწკაპებით, თქვენი მოწყობილობები სტანდარტულ კონფიგურაციაზე დააყენოთ.

რჩევა 3: განაახლეთ თქვენი მოწყობილობა

არ აქვს მნიშვნელობა რომელ ტელეფონსა თუ ტაბლეტს იყენებს თქვენი ორგანიზაცია, მნიშვნელოვანია, რომ ისინი ყოველთვის განახლებული იყოს. ყველა მწარმოებელი (მაგალითად, Windows, Android, iOS) აანონსებს რეგულარულ განახლებულ ვერსიებს, რომლებიც შეიცავს უსაფრთხოების კრიტიკულ ფუნქციებს მოწყობილობის დასაცავად. პროცესი საკმაოდ სწრაფი, მარტივი და უფასოა. ასეთ დროს, სასურველია, მოწყობილობა დაყენებული იყოს ავტომატური განახლების რეჟიმზე. დარწმუნდით, რომ თქვენმა თანამშრომლებმა იციან, რამდენად მნიშვნელოვანია აღნიშნული განახლებები და აუცილებლობის შემთხვევაში, აუხსენით, როგორ განაახლონ მოწყობილობა. გარკვეული დროის შემდეგ განახლებები აღარ იქნება ხელმისაწვდომი (რადგან მოწყობილობა მიაღწევს მხარდაჭერილი სიცოცხლის ციკლის

ბოლოს ეტაპს - end of life), რა დროსაც აუცილებელია ძველი მოწყობილობა თანამედროვე ალტერნატივით შეცვალოთ.

რჩევა 4: განაახლეთ თქვენი აპლიკაციები

ისევე, როგორც თქვენი ორგანიზაციის მოწყობილობებზე არსებული ოპერაციული სისტემები, დაინსტალირებული ყველა აპლიკაციაც ასევე რეგულარულად უნდა განახლდეს პროგრამული უზრუნველყოფის მწარმოებლის პატჩებით. ეს განახლებები არამარტო დაამატებს ახალ ფუნქციებს, ასევე გამოასწორებს უსაფრთხოებასთან დაკავშირებულ ნებისმიერ შეფერხებას. დარწმუნდით, რომ პერსონალმა იცის, როგორ და როდის განაახლონ მოწყობილობები.

რჩევა 5: არ დაუკავშირდეთ უცნობ Wi-Fi Hotspot-ებს

როდესაც საჯარო Wi-Fi-ს იყენებთ (მაგალითად, სასტუმროებში ან რესტორნებში), არ არსებობს მარტივი გზა იმის გასარკვევად, თუ ვინ აკონტროლებს ინტერნეტს. თუ თქვენ დაუკავშირდებით ქსელს, დაინტერესებულ მხარეს შეიძლება წვდომა ჰქონდეს:

- რაზე მუშაობთ ქსელთან კავშირის დროს;
- თქვენი მომხმარებლის სახელი და პაროლი, რომლებსაც სისტემაში ყოფნისას ბევრი აპლიკაცია და ვებ-სერვისი ინახავს.

უმარტივესი უსაფრთხოების ზომაა არ დაუკავშირდეთ ინტერნეტს უცნობი Wi-Fi-ს გამოყენებით, არამედ გამოიყენოთ თქვენი მობილური 3G ან 4G მობილური ქსელი, რომელსაც ექნება ჩაშენებული უსაფრთხოება. ეს ნიშნავს, რომ ასევე შეგიძლიათ გამოიყენოთ „tethering“ (სადაც თქვენი სხვა მოწყობილობები 3G/4G კავშირს იზიარებენ), ან უკაბელო „dongle“ მოწოდებული თქვენი მობილური ქსელით (მაგალითად, უკაბელო MiFi modem). ასევე, შეგიძლიათ გამოიყენოთ ვირტუალური პირადი ქსელები

(VPN), რომელიც ინტერნეტში გაგზავნამდე თქვენს მონაცემებს დაშიფრავს. თუ იყენებთ მესამე მხარის VPN-ებს, აუცილებელია

გადაამოწმოთ, რამდენად სანდოა პროვაიდერი და თავად დააკონფიგუროთ იგი.

### 1.4.4. ნაბიჯი 4 - პაროლების გამოყენება თქვენი მონაცემების დასაცავად

ლეპტოპები, კომპიუტერები, ტაბლეტები და სმარტფონები შეიცავს თქვენი ბიზნესისთვის მნიშვნელოვან უამრავ მონაცემს - კლიენტების პერსონალურ ინფორმაციას და ასევე დეტალებს იმ ონლაინ ანგარიშების შესახებ, რომლებზეც წვდომა გაქვთ. აუცილებელია, რომ ეს მონაცემები თქვენთვის ხელმისაწვდომი იყოს, მაგრამ არა არაავტორიზებული მომხმარებლებისთვის.

**პაროლები,** სწორად დანერგვის შემთხვევაში, უფასო, მარტივ და ეფექტურ გზას წარმოადგენს არაავტორიზებული მომხმარებლების თქვენს მოწყობილობებზე წვდომის თავიდან ასაცილებლად. წინამდებარე თავებში მოცემულია 5 რჩევა, რაც უნდა გახსოვდეთ პაროლების გამოყენებისას.

რჩევა 1: დარწმუნდით, რომ ჩართეთ პაროლით დაცვა

დააყენეთ ეკრანის დაბლოკვის პაროლი, PIN ან ავთენტიფიკაციის სხვა მეთოდი (როგორიცაა თითის ანაბეჭდი ან სახით განბლოკვა). თუ ძირითადად თითის ანაბეჭდს ან სახით განბლოკვას იყენებთ, პაროლს ნაკლებად ხშირად შეიყვანთ, ამიტომ იფიქრეთ გრძელი პაროლის დაყენებაზე, რომლის გამოცნობაც რთული იქნება.

პაროლით დაცვა არ არის მხოლოდ სმარტფონებისა და ტაბლეტებისთვის. დარწმუნდით, რომ თქვენი საოფისე აღჭურვილობა (ასევე, ლეპტოპები და კომპიუტერები) დაშიფვრის ინსტრუმენ-

ტებს იყენებს (როგორიცაა BitLocker Windows-ისთვის), სანდო პლატფორმის მოდულის (TPM) საშუალებით ან FileVault macOS-ზე. თანამედროვე მოწყობილობების უმეტესობას აქვს ჩაშენებული დაშიფვრის ფუნქცია, მაგრამ დაშიფვრისთვის შეიძლება მაინც საჭირო გახდეს ფუნქციის ჩართვა და კონფიგურაცია.

### რჩევა 2: გამოიყენეთ ორნაბიჯიანი დადასტურება „მნიშვნელოვანი“ ანგარიშებისთვის

აუცილებელია გამოიყენოთ ორნაბიჯიანი დადასტურება (ცნობილი, როგორც 2 step verification – 2SV) თქვენი ნებისმიერი ანგარიშისთვის, სადაც ამის ფუნქციონალი არსებობს. აღნიშნული მნიშვნელოვნად აუმჯობესებს თქვენს უსაფრთხოებას, ზედმეტი ძალისხმევის გარეშე. 2SV მოითხოვს ორ განსხვავებულ მეთოდს თქვენი ვინაობის „დასამტკიცებლად“. შესაბამისად, სანამ სასურველ სისტემაში შეხვალთ, როგორც წესი, მოგიწევთ შეიყვანოთ პაროლი და ერთი სხვა მონაცემი. ეს შეიძლება იყოს თქვენს სმარტფონზე გამოგზავნილი კოდი (ან კოდი, რომელიც გენერირებულია ბანკის ბარათის წამკითხველიდან), რომელიც პაროლთან ერთად უნდა შეიყვანოთ.

### რჩევა 3: მოერიდეთ პროგნოზირებადი პაროლების გამოყენებას

თუ თქვენ პასუხისმგებელი ხართ თქვენი ორგანიზაციის IT პოლიტიკაზე, დარწმუნდით, რომ პაროლების შესახებ ინფორმაცია პერსონალს მიეწოდება ისეთი ფორმით, რომელიც მათთვის ადვილად აღსაქმელი და გასაგებია.

პაროლები ადვილად დასამახსოვრებელი უნდა იყოს, მაგრამ სხვისთვის რთული გამოსაცნობი. ამასთან დაკავშირებით, არსებობს კარგი წესი: „დარწმუნდით, რომ ვინმემ, ვინც კარგად გიცნობთ, თქვენს პაროლს 20 მცდელობაში ვერ გამოიცნობს“. პერსონალი ასევე უნდა მოერიდოს ყველაზე გავრცელებული

პაროლების გამოყენებას, რომელთა გამოცნობა კრიმინალებს შეუძლიათ.

გახსოვდეთ, რომ თქვენმა IT სისტემებმა არ უნდა მოსთხოვოს პერსონალს ანგარიშების ან პაროლების გაზიარება სამუშაოს შესასრულებლად. დარწმუნდით, რომ თითოეულ მომხმარებელს აქვს პერსონალური წვდომა წინასწარგანსაზღვრულ სისტემებზე და რომ მინიჭებული წვდომის დონე ყოველთვის არის ყველაზე დაბალი (least privilege approach), რაც მათი საქმის შესასრულებლად არის საჭირო. შეამცირეთ ზედმეტი წვდომა იმ სისტემებზე, რომლებიც არ სჭირდებათ თქვენს თანამშრომლებს.

რჩევა 4: დაეხმარეთ თქვენს პერსონალს გაუმკლავდეს „პაროლის გადატვირთვას“

თუ საკუთარ ორგანიზაციაში პასუხისმგებელი ხართ პაროლების გამოყენებაზე, არსებობს რამდენიმე გამოსავალი, რაც გააუმჯობესებს ორგანიზაციის უსაფრთხოებას. რაც მთავარია, თქვენს თანამშრომლებს არ ექნებათ ათობით არასამუშაო პაროლი დასამახსოვრებელი. არ არის აუცილებელი პაროლები რეგულარულად შეიცვალოს ისეთ სერვისებზე, რომლებსაც მომხმარებელი არ იყენებს. შეცვალეთ პაროლები ისეთ სისტემებზე, რომლებსაც მომხმარებელი აქტიურად იყენებს. ასევე, გაითვალისწინეთ, რომ პაროლის შეცვლა აუცილებელია იმ შემთხვევაში, თუ არსებობს ეჭვი, რომ ეს პაროლი კომპრომიტირებულია.

თქვენ ასევე უნდა დანერგოთ პაროლების მენეჯერი (პაროლების საცავი), რათა პერსონალმა შეძლოს მნიშვნელოვანი ანგარიშების (როგორიცაა ელექტრონული ფოსტა და საბანკო მომსახურება) პაროლების უსაფრთხო შენახვა. როგორც წესი, თანამშრომლებს პაროლები ხშირად ავიწყდებათ, ამიტომ დარწმუნდით, რომ მათ შეუძლიათ ადვილად შეცვალონ საკუთარი პაროლები.

რჩევა 5: შეცვალეთ ყველა ნაგულისხმევი პაროლი

ერთ-ერთი ყველაზე გავრცელებული შეცდომაა მწარმოებლების ნაგულისხმევი პაროლების (default passwords) გამოყენება, რომლითაც სმარტფონები, ლეპტოპები და სხვა ტიპის აღჭურვილობა გაიცემა. შეცვალეთ ყველა ნაგულისხმევი პაროლი, სანამ მოწყობილობები პერსონალს გადაეცემა. თქვენ ასევე რეგულარულად უნდა შეამოწმოთ მოწყობილობები (და პროგრამული უზრუნველყოფა) უცვლელი ნაგულისხმევი პაროლების გამოსავლენად.

### 1.4.5. ნაბიჯი 5 - ფიშინგის შეტევების თავიდან აცილება

როგორც წესი, ფიშინგის შეტევისას, თაღლითები აგზავნიან ყალბ წერილებს ათასობით ადამიანთან და ითხოვენ სენსიტიური ინფორმაციის (როგორიცაა საბანკო დეტალები) გაცემას ან მავნე ბმულებზე გადასვლას. შემტევი შეიძლება თქვენს მოტყუებას შეეცადოს ფულის გაგზავნის ან თქვენი ანგარიშების (accounts) დეტალების მოპოვების მიზნით. ასევე, შემტევს შესაძლებელია ჰქონდეს პოლიტიკური თუ იდეოლოგიური მოტივი ორგანიზაციის შესახებ ინფორმაციაზე წვდომის მისაღებად.

ფიშინგული ელექტრონული ფოსტის დაფიქსირება სულ უფრო რთული ხდება. როგორიც არ უნდა იყოს თქვენი ორგანიზაცია/ბიზნესი, რაღაც მომენტში მაინც გახდებით ფიშინგ შეტევის მსხვერპლი. წინამდებარე თავი შეიცავს რამდენიმე მარტივ ნაბიჯს, რომელიც დაგეხმარებათ ყველაზე გავრცელებული ფიშინგის შეტევების იდენტიფიცირებაში.

რჩევა 1: დააკონფიგურირეთ ანგარიშები წარმატებული შეტევების გავლენის შესამცირებლად

თქვენ უნდა დააკონფიგურიროთ თქვენი პერსონალის ანგარიშები წინასწარ „მინიმალური პრივილეგიის“ პრინციპის გა-

მოყენებით. ეს ნიშნავს იმას, რომ პერსონალს უნდა მიეცეს მომხმარებლის უფლებების ყველაზე დაბალი დონე, რომელიც მათი სამუშაოს შესასრულებლად საკმარისი იქნება. შესაბამისად, იმ შემთხვევაშიც, თუ ისინი გახდებიან ფიშინგის შეტევის მსხვერპლი, პოტენციური ზიანი მცირდება. მავნე პროგრამით ან ანგარიშში შესვლის დეტალების დაკარგვით გამოწვეული ზიანის შემდგომში შემცირების მიზნით, დარწმუნდით, რომ თქვენი თანამშრომლები არ იყენებენ ინტერნეტს ან არ ამოწმებენ წერილებს ადმინისტრატორის უფლებების მქონე ანგარიშიდან. ადმინისტრატორის ანგარიში არის მომხმარებლის ანგარიში, რომელიც საშუალებას გაძლევთ განახორციელოთ ცვლილებები, რომლებიც გავლენას მოახდენს სხვა მომხმარებლებზე. ადმინისტრატორებს შეუძლიათ შეცვალონ უსაფრთხოების პარამეტრები, დააინსტალირონ პროგრამული უზრუნველყოფა და აპარატურა და წვდომა მიიღონ კომპიუტერზე არსებულ ყველა ფაილზე. ასე რომ, თავდამსხმელი, რომელსაც ადმინისტრატორის ანგარიშზე არაავტორიზებული წვდომა აქვს, შეიძლება ბევრად უფრო საზიანო იყოს, ვიდრე სტანდარტული მომხმარებლის ანგარიშზე წვდომის შემთხვევაში.

გამოიყენეთ ორფაქტორიანი ავთენტიფიკაცია (2FA) ისეთ მნიშვნელოვან ანგარიშებზე, როგორიცაა ელექტრონული ფოსტა. ამ მეთოდის გამოყენებით, მაშინაც კი, თუ თავდამსხმელმა იცის თქვენი პაროლი, ის მაინც ვერ შეძლებს ანგარიშზე წვდომის მიღება.

რჩევა 2: იფიქრეთ იმაზე, თუ როგორ მუშაობთ

იფიქრეთ იმაზე, თუ როგორ შეიძლება ვინმემ თქვენი ორგანიზაცია მიზანში ამოიღოს და დარწმუნდით, რომ თანამშრომლებს ესმით მუშაობის ნორმალური გზები (განსაკუთრებით სხვა ორგანიზაციებთან ურთიერთობისას), რათა

ისინი უკეთესად იყვნენ მომზადებულნი იმისათვის, რომ შეამჩნიონ გამონაკლისი/ანომალიური მოთხოვნები.

გავრცელებული მეთოდები მოიცავს იმ სერვისის ინვოისის გაგზავნას, რომელიც არ გამოგიყენებიათ, ასე რომ, როდესაც დანართი იხსნება, მავნე პროგრამა ავტომატურად დაინსტალირდება თქვენს კომპიუტერში. მეორე გახლავთ პერსონალის მოტყუება ელექტრონული ფოსტის დახმარებით, ფულის გადარიცხვის ან ორგანიზაციის შესახებ ინფორმაციის მიღების მიზნით. იფიქრეთ თქვენს ჩვეულ სამუშაო პრაქტიკაზე და იმაზე, თუ როგორ შეიძლება ზემოხსენებული ხრიკების ამოცნობა. მაგალითად:

- იციან თუ არა თანამშრომლებმა რა გააკეთონ მეილზე მიღებულ უჩვეულო თხოვნებზე და სად მიიღონ დახმარება?
- ჰკითხეთ საკუთარ თავს, საჭიროა თუ არა ელექტრონული ფოსტით მიღებული მოთხოვნის დასადასტურებლად მენეჯერის ჩართვა?
- კარგად გესმით თქვენი რეგულარული საქმიანი ურთიერთობები? თაღლითები ხშირად აგზავნიან ფიშინგ წერილებს დიდი ორგანიზაციებიდან (როგორიცაა ბანკები) იმ იმედით, რომ ელექტრონული ფოსტის ზოგიერთ მიმღებს კავშირი ექნება ამ კომპანიასთან. თუ მიიღებთ ელექტრონულ ფოსტას ისეთი ორგანიზაციისგან, რომელთანაც არ გაკავშირებთ საქმიანი ურთიერთობა, აუცილებლად გადაამოწმეთ.
- იფიქრეთ იმაზე, თუ როგორ შეგიძლიათ წაახალისოთ და მხარი დაუჭიროთ თქვენს თანამშრომლებს, რათა გაუჩნდეთ კითხვები საეჭვო ან უბრალოდ უჩვეულო მოთხოვნების მიმართ - მაშინაც კი, თუ ისინი მნიშვნელოვანი პიროვნე-

ბებისგან მოდის (მაგალითად, კომპანიის დამფუძნებელი ან ორგანიზაციის ხელმძღვანელი).

რჩევა 3: შეამოწმეთ ფიშინგის აშკარა ნიშნები

მოლოდინი, რომ თანამშრომლები შეძლებენ ამოიცნონ და წაშალონ ყველა ფიშინგული ელექტრონული წერილი - შეუძლებელია და დიდ უარყოფით გავლენას მოახდენს ორგანიზაციის/ბიზნესის პროდუქტიულობაზე. თუმცა, ბევრი ფიშინგის მცდელობა მაინც ერგება ტრადიციული თავდასხმის ფორმას, ამიტომ მოძებნეთ შემდეგი გამაფრთხილებელი ნიშნები:

- ბევრი ფიშინგის თაღლითობა წარმოიქმნება საზღვარგარეთ და ხშირად მართლწერა, გრამატიკა და პუნქტუაცია ცუდია. ზოგჯერ შემტევები ცდილობენ შექმნან ოფიციალური სახის ელექტრონული წერილები ლოგოებისა და გრაფიკის ჩათვლით. ამიტომ კარგად გადაამოწმეთ, შესაბამისია თუ არა გამოგზავნილი წერილის დიზაინი და მართლწერის ფორმები.
- თუ სახელით არ მოგმართავენ და იყენებენ სტანდარტულ მიმართვას - „ძვირფასო მომხმარებელო“, „მეგობარო“ ან „კოლეგავ“? ეს შეიძლება იყოს იმის ნიშანი, რომ გამომგზავნი რეალურად არ გიცნობთ, რაც ასევე ფიშინგის თაღლითობის ნაწილს წარმოადგენს.
- დააკვირდით, შეიცავს თუ არა ელექტრონული ფოსტა ისეთ ფრაზებს, რომელიც თქვენს სასწრაფო მოქმედებას მოითხოვს. ფიშინგის დროს ხშირად გამოიყენება ფრაზები - "გაგზავნეთ ეს დეტალები 24 საათის განმავლობაში" ან "თქვენ იყავით დანაშაულის მსხვერპლი, დააწკაპეთ აქ დაუყოვნებლივ".
- დააკვირდით ელექტრონულ ფოსტას, რომელიც, როგორც ჩანს, მოვიდა თქვენი ორგანიზაციის მაღალი რანგის

პირისგან და თანხის გადახდა ხდება კონკრეტულ საბანკო ანგარიშზე. შეხედეთ გამომგზავნის სახელს. ლეგიტიმურად ჟღერს თუ ცდილობს ვინმეს მიბაძვას?

- თუ წერილი ზედმეტად კარგად ჟღერს. მაგალითად, ნაკლებად სავარაუდოა, რომ ვინმეს თქვენთვის ფულის მოცემა სურდეს უსაფუძვლოდ.

ელექტრონული ფოსტის ფილტრაციის სერვისები ცდილობენ გაგზავნონ ფიშინგ წერილები სპამის საქაღალდეებში, თუმცა წესები, რომლებიც ფილტრაციას განსაზღვრავს, თქვენი ორგანიზაციის საჭიროებებს უნდა ერგებოდეს. თუ წესები ძალიან ღია და საეჭვოა, ელექტრონული ფოსტა არ გაიგზავნება სპამის/უსარგებლო საქაღალდეებში. ასეთ შემთხვევაში, მომხმარებლებს მოუწევთ მართონ ელექტრონულ ფოსტაზე შემოსული წერილების დიდი რაოდენობა, რაც მათი მხრიდან გარკვეულ ენერგიას მოითხოვს. ხოლო თუ წესები ძალიან მკაცრია, ზოგიერთი ლეგიტიმური ელექტრონული წერილი შეიძლება დაიკარგოს. ამიტომ, დროთა განმავლობაში, შეიძლება დაგჭირდეთ წესების შეცვლა კომპრომისის უზრუნველსაყოფად.

რჩევა 4: შეატყობინეთ ყველა თავდასხმა

დარწმუნდით, რომ თქვენი თანამშრომლები წახალისებულნი არიან, შეატყობინონ შესაბამის სტრუქტურულ ერთეულს ან პასუხისმგებელ პირ პოტენციური შეტევის შესახებ. ასეთ დროს, მნიშვნელოვანია, რაც შეიძლება მალე მიიღოთ ზომები მავნე პროგრამების სკანირებისთვის და პაროლების შესაცვლელად.

არ დასაჯოთ თანამშრომლები, თუ ისინი დააჭერენ ფიშინგ მეილს. ეს ხელს შეუშლის ადამიანებს მომავალში დარეპორტებისგან და შეიძლება მათ იმდენად შეეშინდეთ, რომ ზედმეტი

დრო და ენერგია დახარჯონ ყოველი ელექტრონული ფოსტის შესასწავლად. ეს ორი რამ უფრო მეტ ზიანს აყენებს თქვენს ბიზნესს გრძელვადიან პერსპექტივაში.

რჩევა 5: შეამოწმეთ თქვენი ციფრული კვალი

თავდამსხმელები იყენებენ საჯაროდ ხელმისაწვდომ ინფორმაციას თქვენი ორგანიზაციისა და პერსონალის შესახებ, რათა მათი ფიშინგული შეტყობინებები უფრო დამაჯერებელი გახადონ. ისინი აღნიშნული ინფორმაციას ორგანიზაციის ვებ საიტიდან და სოციალური მედიის ანგარიშებიდან იღებენ (ინფორმაცია, რომელიც ცნობილია როგორც „ციფრული კვალი“).

- გაიგეთ თქვენი ორგანიზაციის ვებ საიტზე და სოციალური მედიის გვერდებზე გაზიარებული ინფორმაციის გავლენა. რა უნდა იცოდნენ თქვენი ვებ საიტის ვიზიტორებმა და რა დეტალებია არასაჭირო (მაგრამ შეიძლება სასარგებლო იყოს თავდამსხმელებისთვის)?
- იცოდეთ, რა ინფორმაციას გასცემენ ონლაინ თქვენი პარტნიორები, კონტრაქტორები და მომწოდებლები ორგანიზაციის შესახებ.
- დაეხმარეთ თქვენს თანამშრომლებს იმის გააზრებაში, თუ რა გავლენა შეიძლება იქონიოს მათზე და თქვენს ორგანიზაციაზე პირადი ინფორმაციის გაზიარებამ. ეს არ ნიშნავს იმას, რომ ადამიანებმა ინტერნეტიდან საკუთარი თავის შესახებ ყველა კვალი უნდა წაშალონ. მნიშვნელოვანია, მხარი დაუჭიროთ მათ, როდესაც ისინი მართავენ თავიანთ ციფრულ კვალს, ქმნიან პროფილს, რომელიც მათთვის და ორგანიზაციისთვის იმუშავებს.

# 2. თემატური მაგალითები

## 2.1. პერსონალური მონაცემების დაცვა - რა უნდა ვიცოდეთ

### 2.1.1. რა არის ჩემი პერსონალური მონაცემები?

საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ განსაზღვრავს, რომ პერსონალური მონაცემები არის ნებისმიერი სახის ინფორმაცია, რომლითაც შესაძლებელია პირის იდენტიფიცირება. მაგალითად: თქვენი სახელი, გვარი, პირადი ნომერი, ფოტო, ვიდეო ჩანაწერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, სოციალური ქსელის ანგარიში, პირადი მიმოწერა. პერსონალური მონაცემია ასევე ინფორმაცია თქვენი სამუშაო ადგილის, შემოსავლების, ოჯახური მდგომარეობის შესახებ და სხვა.

ასევე, არსებობს განსაკუთრებული კატეგორიის პერსონალური მონაცემებიც. აღნიშნულ კატეგორიას მიეკუთვნება ინფორმაცია, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული კავშირის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, აღკვეთის ღონისძიების შეფარდებასთან, საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან. დამატებით, განსაკუთრებულ კატეგორიაში შედის ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა.

საქართველოს მოქმედი კანონმდებლობა ადგენს განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის უფრო მაღალ სტანდარტს და ასევე, წესების დარღვევისას, სანქცირების მექანიზმებიც უფრო მკაცრია, ვიდრე სტანდარტული პერსონალური მონაცემების შემთხვევაში.

### 2.1.2. რას ნიშნავს პერსონალური მონაცემების უკანონო დამუშავება?

საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ განსაზღვრავს, რომ მონაცემთა დამუშავება არის ნებისმიერი ქმედება, რომელიც პერსონალური მონაცემების მიმართ ხორციელდება: შეგროვება, ჩაწერა, შენახვა, გამოყენება, გამჟღავნება, ფოტოზე აღბეჭდვა, მესამე პირისთვის გადაცემა, გავრცელება, წაშლა, განადგურება და სხვა.

მოქალაქის პერსონალურ მონაცემებს შეიძლება ამუშავებდეს ნებისმიერი საჯარო თუ კერძო ორგანიზაცია, რომელთანაც მოქალაქეს აქვს ურთიერთობა. მაგალითად:

- სუპერმარკეტების ქსელი ამუშავებს მოქალაქის პერსონალურ მონაცემებს, როდესაც მოქალაქე ლოიალობის ბარათს არეგისტრირებს.
- კლინიკა ამუშავებს მოქალაქის პერსონალურ მონაცემებს, როდესაც ატარებს დიაგნოსტირებას, გამოკვლევებს, აწარმოებს სამედიცინო ისტორიას.
- სოციალური ქსელი ამუშავებს მოქალაქის (მომხმარებლის) პერსონალურ მონაცემებს, როდესაც აქვეყნებს საკუთარ ფოტოს ან რეგისტრაციის მიზნით, შესაბამის ველში ელექტრონული ფოსტის მისამართი და პაროლი შეჰყავს.
- საგანმანათლებლო დაწესებულება ამუშავებს სტუდენტის პერსონალურ მონაცემებს, როდესაც სტუდენტი ეწერება

სასწავლო კურსზე, რისთვისაც საკუთარ პირად ნომერს, სახელს და გვარს უთითებს.

ყველა ორგანიზაცია, რომელსაც შეხება აქვს მოქალაქის პერსონალურ მონაცემებთან, მონაცემთა დამმუშავებელია, ხოლო მოქალაქე კი - მონაცემთა სუბიექტი.

პერსონალურ მონაცემთა სენსიტიურობის გათვალისწინებით, საქართველოს მოქმედი კანონმდებლობა ადგენს წესებს, პრინციპებს, საფუძვლებსა და უსაფრთხოების ზომებს, რომელიც მონაცემთა დამმუშავებელმა მონაცემების დამუშავებისას აუცილებლად უნდა დაიცვას. ამ წესების დარღვევით მონაცემთა შეგროვება, შენახვა, გამოყენება და გავრცელება კანონდარღვევაა.

### 2.1.3. მონაცემთა დამუშავების საფუძვლები

მონაცემთა დამუშავება დასაშვებია, თუ:

- **არსებობს მონაცემთა სუბიექტის თანხმობა -** პირის ნებაყოფლობითი, ინფორმირებული და მკაფიოდ გამოხატული თანხმობა მისი პერსონალური მონაცემების დამუშავებაზე. მაგალითად:
  - საიტზე რეგისტრაციისას ან აპლიკაციის გადმოწერისას - დათანხმება ვებგვერდზე განთავსებულ კონფიდენციალურობის პოლიტიკაზე;
  - სამედიცინო ანკეტის ან ლოიალობის ბარათის გახსნისას - ხელმოწერა ხელშეკრულებაზე.
- **მონაცემთა დამუშავება გათვალისწინებულია კანონით -** რიგ შემთხვევებში, სხვადასხვა საკანონმდებლო აქტი ითვალისწინებს მოქალაქის შესახებ პერსონალური მონაცემების დამუშავების საჭიროებას;

- **მონაცემთა დამუშავება საჭიროა მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად -** მაგალითად, საგადასახადო მიზნებით მონაცემთა გარკვეული ვადით შენახვა;
- **მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად -** მაგალითად, თუ საგანგებო სიტუაციის დროს ადამიანის სიცოცხლეს საფრთხე ემუქრება და მის გადასარჩენად აუცილებელია ადგილმდებარეობის დადგენა;
- **მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად,** გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლების დაცვის აღმატებული ინტერესი;
- მონაცემები საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა. მაგალითად:
    - სოციალურ ქსელში საჯაროდ განთავსებული ფოტო;
    - ონლაინ ვაჭრობის პლატფორმებზე საჯაროდ განთავსებული საკონტაქტო ინფორმაცია;
- **მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად -** მაგალითად, დანაშაულის პრევენცია, საკუთრების ან არასრულწლოვნების მავნე ზეგავლენისაგან დაცვის მიზნით;
- **მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად ან მისთვის**

მომსახურების გასაწევად.

განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ მონაცემთა სუბიექტის წერილობითი თანხმობით ან იმ შემთხვევებში, როცა:

- ნასამართლობასთან და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებების და ურთიერთობის ხასიათიდან გამომდინარე, მათ შორის, დასაქმების თაობაზე გადაწყვეტილების მისაღებად;
- მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არა აქვს, მონაცემთა დამუშავებაზე თანხმობა განაცხადოს;
- მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე, თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის;
- მონაცემთა სუბიექტმა საჯარო გახადა მის შესახებ მონაცემები მათი გამოყენების აშკარა აკრძალვის გარეშე;
- მონაცემები მუშავდება პოლიტიკური, ფილოსოფიური, რელიგიური ან პროფესიული გაერთიანების ან არაკომერციული ორგანიზაციის მიერ ლეგიტიმური საქმიანობის განხორციელებისას. ასეთ შემთხვევაში მონაცემთა დამუშავება შეიძლება დაკავშირებული იყოს მხოლოდ ამ გაერთიანების/ორგანიზაციის წევრებთან ან პირებთან,

რომლებსაც მუდმივი კავშირი აქვთ ამ გაერთიანებასთან/ორგანიზაციასთან.

- ხდება მონაცემთა დამუშავება ბრალდებულთა/მსჯავრდებულთა პირადი საქმეებისა და რეესტრების წარმოების, მსჯავრდებულის მიმართ მის მიერ სასჯელის მოხდის ინდივიდუალური დაგეგმვის ან/და მსჯავრდებულის სასჯელის მოხდისგან პირობით ვადამდე გათავისუფლებასთან და მისთვის სასჯელის მოუხდელი ნაწილის უფრო მსუბუქი სახის სასჯელით შეცვლასთან დაკავშირებული საკითხების განხილვის მიზნით.
- მონაცემები მუშავდება „არასაპატიმრო სასჯელთა აღსრულების წესისა და პრობაციის შესახებ“ საქართველოს კანონის მე-2 მუხლით გათვალისწინებული სამართლებრივი აქტების აღსრულების მიზნით.
- მონაცემები მუშავდება „საერთაშორისო დაცვის შესახებ“ საქართველოს კანონით პირდაპირ გათვალისწინებულ შემთხვევებში.
- მონაცემები მუშავდება მიგრაციის მონაცემთა ერთიანი ანალიტიკური სისტემის ფუნქციონირებისათვის.
- მონაცემები მუშავდება სპეციალური საგანმანათლებლო საჭიროების მქონე პირთა განათლების უფლების რეალიზების მიზნით.

### 2.1.4. მონაცემთა დამუშავების პრინციპები

პერსონალური მონაცემების დამუშავებისას, აუცილებელია გათვალისწინებული იქნეს შემდეგი პრინციპები:

- **სამართლიანობა და კანონიერება** - პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიე-

რად, პიროვნების ღირსების შეულახავად;

- **მკაფიოდ განსაზღვრული კანონიერი მიზნის არსებობა -** აუცილებელია, არსებობდეს კონკრეტული მიზანი, რისთვისაც ხდება მონაცემთა დამუშავება. სხვა მიზნებით მონაცემების გამოყენება დაუშვებელია.
- **პროპორციულობა და ადეკვატურობა -** მონაცემები უნდა დამუშავდეს იმ მინიმალური მოცულობით, რაც აუცილებელია მონაცემთა დამუშავების კონკრეტული მიზნის მისაღწევად. თავად მონაცემებიც, ამ მიზნის შესაბამისი უნდა იყოს.
- **ნამდვილობა და სიზუსტე -** მონაცემები უნდა იყოს ნამდვილი და ზუსტი, საჭიროების შემთხვევაში, უნდა განახლდეს, ასევე, უნდა გადამოწმდეს ინფორმაციის წყაროს სანდოობა, გასწორდეს მცდარი და არაზუსტი მონაცემები;
- **შენახვის ვადა - პერსონალური** მონაცემები უნდა ინახებოდეს კანონით განსაზღვრული ვადით ან იმ ვადით, რაც აუცილებელია მიზნის მისაღწევად. მიზნის მიღწევის შემდეგ, ისინი უნდა წაიშალოს, ან შეინახოს პირის იდენტიფიცირების გამომრიცხავი ფორმით.

<u>თუ ჩათვლით, რომ ორგანიზაციას არ აქვს თქვენი მონაცემების დამუშავების სამართლებრივი საფუძველი ან არღვევს კანონით განსაზღვრულ რომელიმე პრინციპს, შეგიძლიათ მიმართოთ პერსონალურ მონაცემთა დაცვის სამსახურს ან სასამართლოს.</u>

დარღვევის დადგენის შემთხვევაში, „პერსონალური მონაცემების დაცვის შესახებ“ კანონი განსაზღვრავს ადმინის-

ტრაციულ პასუხისმგებლობას გაფრთხილების ან ჯარიმის სახით.

### 2.1.5. როგორ გამოვითხოვო ჩემს შესახებ ინფორმაცია?

- პერსონალური მონაცემების დამუშავების შესახებ ინფორმაციის მოთხოვნა შეგიძლიათ როგორც ზეპირი, ისე წერილობითი ფორმით.
- თქვენ გაქვთ უფლება, გაეცნოთ თქვენ შესახებ საჯარო დაწესებულებაში არსებულ პერსონალურ მონაცემებს და უსასყიდლოდ მიიღოთ ამ მონაცემების ასლები, გარდა იმ მონაცემებისა, რომელთა გაცემისათვის საქართველოს კანონმდებლობით გათვალისწინებულია საფასური.
- მნიშვნელოვანია იცოდეთ, რომ თქვენ გაქვთ უფლება, მოითხოვოთ ინფორმაცია მხოლოდ თქვენი პერსონალური მონაცემების შესახებ. სხვა პირის მონაცემების დამუშავების შესახებ ინფორმაციის მოთხოვნისთვის აუცილებელია სპეციალური უფლებამოსილების ან წარმომადგენლობის დადასტურება, მაგალითად, მშობლის მიერ შვილის ან ადვოკატის მიერ კლიენტის მონაცემების შესახებ ინფორმაციის მოთხოვნის შემთხვევაში.

### 2.1.6. პერსონალური მონაცემების გასწორება, წაშლა ან განახლება

თუ სუბიექტის პერსონალური მონაცემები არასრულია, არაზუსტია, არ არის განახლებული ან თუ მათი შეგროვება და დამუშავება განხორციელდა კანონის მოთხოვნების დარღვევით, სუბიექტს უფლება აქვს მოითხოვოთ მათი გასწორება, განახლება, დამატება, დაბლოკვა (მონაცემთა დამუშავების დროებითი შეჩერება), წაშლა ან განადგურება.

მოთხოვნის სასურველ ფორმას სუბიექტი თავად ირჩევს. ამის გა-

კეთება შესაძლებელია როგორც ზეპირად, ასევე წერილობითი ფორმით. მონაცემთა დამმუშავებელი კი ვალდებულია დააკმაყოფილოს მოთხოვნა მისი მიღებიდან 15 დღის ვადაში ან აცნობოს სუბიექტს მოთხოვნის დაკმაყოფილებაზე უარის თქმის საფუძველი.

### 2.1.7. პირდაპირი მარკეტინგის მიზნით პერსონალური მონაცემების დამუშავება

პირდაპირი მარკეტინგი არის მომხმარებლისთვის მოკლე ტექსტური შეტყობინებით, საფოსტო გზავნილით, სატელეფონო ზარით, ელექტრონული ფოსტით ან უშუალო კომუნიკაციით საქონლის, მომსახურებისა და დასაქმების შეთავაზება.

პირდაპირი მარკეტინგის მიზნებისთვის მონაცემები შეიძლება დამუშავდეს, თუ:

- მოქალაქემ განაცხადა წერილობითი თანხმობა;
- ინფორმაცია ხელმისაწვდომია საჯაროდ ან ორგანიზაცია კანონიერად ფლობს ამ მონაცემებს.

ხშირად პერსონალური მონაცემების, მათ შორის, საკონტაქტო ინფორმაციის გამოყენებაზე კომპანიებს თავად მომხმარებლები თანხმდებიან. მაგალითად, დაგროვებითი ბარათის შევსებისას მაღაზიას ვაძლევთ უფლებას გამოგვიგზავნოს შეტყობინებები, მობილურ ოპერატორს ვრთავთ ნებას გამოიყენოს ჩვენი ტელეფონის ნომერი პარტნიორი კომპანიების მარკეტინგული მიზნებისთვის, ვხდებით რა ბანკის კლიენტი, ვთანხმდებით მას საინფორმაციო და სარეკლამო შეტყობინებების გამოგზავნაზე და სხვა.

კომპანიებს ჩვენი საკონტაქტო ინფორმაციის პირდაპირი მარკეტინგის მიზნით გამოყენება მაშინაც შეუძლიათ, თუ ეს ინ-

ფორმაცია საჯაროდაა გამოქვენებული. მაგალითად, თუ ტელეფონის ნომერი ყიდვა-გაყიდვის საიტზე გაასაჯაროვეთ, ღიად მიუთითეთ ელექტრონული ფოსტა ფეისბუქის გვერდზე და სხვა.

თუმცა, მიუხედავად იმისა, მიეცით თუ არა თანხმობა ორგანიზაციას პირდაპირი მარკეტინგის მიზნებისთვის თქვენი მონაცემების გამოყენებაზე, უნდა გქონდეთ საშუალება, უარი თქვათ მასზე - იმავე ფორმით რა ფორმითაც მოხდა შეთავაზება ან სხვა ხელმისაწვდომი და ადეკვატური საშუალებებით.

მაგალითად, სარეკლამო შეტყობინებას აუცილებლად უნდა ახლდეს უარის თქმის მექანიზმი და მკაფიო მითითება იმაზე, თუ როგორ შეუძლია მოქალაქეს სარეკლამო შეტყობინების მიღების შეწყვეტა - ე.წ. SMS OFF; ელექტრონული ფოსტის შემთხვევაში, წერილს უნდა ახლდეს ე.წ. Unsubscribe მექანიზმი.

თქვენ გაქვთ უფლება მონაცემთა დამმუშავებელს ნებისმიერ დროს და ნებისმიერი ფორმით (ზეპირი, წერილობითი) მოსთხოვოთ, შეწყვიტოს თქვენი მონაცემების პირდაპირი მარკეტინგის მიზნებისთვის გამოყენება. კომპანია ვალდებულია შეწყვიტოს თქვენი მონაცემების პირდაპირი მარკეტინგის მიზნით გამოყენება თქვენი მოთხოვნიდან 10 სამუშაო დღის ვადაში.

თქვენ გაქვთ უფლება იცოდეთ, რა მონაცემები მუშავდება თქვენ შესახებ და ნებისმიერ დროს მოითხოვოთ მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა ან განადგურება. ასევე, გაქვთ უფლება იცოდეთ, ვინ არის მარკეტინგული საქმიანობის განმახორციელებელი, რა წყაროდან მოიპოვა თქვენი მონაცემები და რა საფუძვლით.

## 2.2. ფიშინგი და ელექტრონული ფოსტის უსაფრთხოება

### 2.2.1. რა არის სოციალური ინჟინერია?

სოციალური ინჟინერია არის მსხვერპლზე მანიპულირების, ზემოქმედების ან მოტყუების ტაქტიკა, რათა შემტევმა მოიპოვოს კონტროლი კომპიუტერულ სისტემაზე, მოიპაროს პირადი ან ფინანსური ინფორმაცია. სოციალური ინჟინერია იყენებს ფსიქოლოგიურ მანიპულაციას, რათა შემტევმა მიიღოს წვდომა სენსიტიურ ინფორმაციაზე ან აიძულოს მსხვერპლი დაარღვიოს უსაფრთხოების წესები/ნორმები.

სოციალური ინჟინერიის შეტევები ხდება ერთ ან რამდენიმე ეტაპად. თავდაპირველად, კიბერკრიმინალი აგროვებს ზოგად ინფორმაციას მსხვერპლის შესახებ, რომელიც დაეხმარება მას პოტენციურად სისტემაში შეღწევის გზებისა და უსაფრთხოების სისუსტეების გამოვლენაში. შემდგომ ეტაპზე, თავდამსხმელი იყენებს პრეტექსტის ისეთ ფორმას, როგორიც არის განსახიერება (impersonation), რათა მსხვერპლის ნდობა მოიპოვოს. აღნიშნული ნდობის საფუძველზე, მსხვერპლი გასცემს სენსიტიურ ინფორმაციას ან/და შემტევს ანიჭებს წვდომას სამიზნე სისტემაზე.

#### სოციალური ინჟინერიის შეტევის სახეები

არსებობს სოციალური ინჟინერიის შეტევების მრავალი განსხვავებული ფორმა, რომელიც შესაძლოა განხორციელდეს ყველგან, სადაც ადამიანია. ქვემოთ მოცემულია სოციალური ინჟინერიის შეტევის გავრცელებული ფორმები.

#### რა არის ფიშინგი?

სანდო სუბიექტად შენიღბვის გზით, ელექტრონული ფოსტის, SMS ტექსტური შეტყობინებების ან ტელეფონით სენსიტიური ინფორმაციის, მათ შორის მომხმარებლის სახელების, პაროლე-

ბისა და საკრედიტო ბარათის დეტალების მოპოვების მცდელობის პროცესს ფიშინგი ეწოდება. ფიშინგ შეტევისას, შემტევი ქმნის გადაუდებლობის, ცნობისმოყვარეობის ან შიშის გრძნობას. ფიშინგ შეტყობინება მსხვერპლს უბიძგებს გასცეს სენსიტიური ინფორმაცია, დააწკაპოს მავნე ვებ საიტის ბმულზე ან გახსნას დანართები, რომლებიც მავნე პროგრამას შეიცავს.

### რა არის ვიშინგი?

Vishing არის სოციალური ინჟინერიის სახეობა, რომელიც ხმოვან კომუნიკაციას იყენებს. ეს ტექნიკა შეიძლება გაერთიანდეს სოციალური ინჟინერიის სხვა ფორმებთან, რომლებიც აიძულებენ მსხვერპლს, დარეკოს გარკვეულ ნომერზე და გაამჟღავნოს სენსიტიური ინფორმაცია. ვიშინგური შეტევები შეიძლება განხორციელდეს მთლიანად ხმოვანი კომუნიკაციების საშუალებით ე.წ. Voice over Internet Protocol (VoIP) გადაწყვეტილებების და სამაუწყებლო სერვისების გამოყენებით. VoIP ადვილად იძლევა აბონენტის იდენტიფიკაციის (ID) გაყალბების საშუალებას, რითაც შეიძლება ისარგებლოს შემტევმა და საზოგადოების ნდობით აღჭურვილი დაწესებულების დასახელება გამოიყენოს. მაგალითად, მსხვერპლის ტელეფონზე შეიძლება შემოვიდეს ზარი, რომელიც იდენტიფიცირდება როგორც რომელიმე საჯარო ან კერძო დაწესებულება, სინამდვილეში კი ეს იყოს შემტევის მიერ განხორციელებული ზარი.

### რა არის სმიშინგი?

Smishing არის სოციალური ინჟინერიის ფორმა, რომელიც იყენებს SMS ან ტექსტურ შეტყობინებებს. ტექსტური შეტყობინებები შეიძლება შეიცავდეს ისეთ ბმულებს, როგორიცაა ვებგვერდები, ელფოსტის მისამართები ან ტელეფონის ნომრები, რომლებზე დაწკაპებითაც შეიძლება ავტომატურად გახსნას ბრაუზერის ფანჯარა, ელექტრონული წერილი ან აკრიფოს ნომერი. ელექ-

ტრონული ფოსტის, ხმის, ტექსტური შეტყობინებისა და ბრაუზერის ფუნქციონალობის ინტეგრაცია ზრდის იმის ალბათობას, რომ მომხმარებელი გახდეს მავნე აქტივობის მსხვერპლი.

### რა არის ბეითინგი (Baiting)?

ბეითინგი (სატყუარა) სოციალური ინჟინერიის შეტევის ტიპია, სადაც თაღლითი მსხვერპლის ხაფანგში შესატყუებლად ცრუ დაპირებას იყენებს, რამაც შეიძლება გამოიწვიოს პერსონალური ან/და ფინანსური ინფორმაციის გაუონვა სისტემაში მავნე პროგრამის მოტყუებით გააქტიურების გზით. როგორც წესი, ბეითინგისას გამოიყენება მავნე კოდის გავრცელება დანართის სახით, რომელსაც მიმზიდველი სახელი აქვს.

ბეითინგის ყველაზე გავრცელებული ფორმა იყენებს ფიზიკურ მედია მატარებელს (მაგ. USB flash drive) მავნე პროგრამების გასავრცელებლად. მაგალითად, შემტევი ტოვებს მავნე პროგრამით ინფიცირებული ფლეშ მეხსიერების ბარათს (სატყუარას) თვალსაჩინო ადგილზე, სადაც პოტენციური მსხვერპლი აუცილებლად ნახავს მას. როდესაც მსხვერპლი გამოიყენებს ფლეშ დრაივს სამუშაო ან სახლის კომპიუტერში, მავნე პროგრამა ავტომატურად დაინსტალირდება სისტემაში.

### რა არის ადევნება (Tailgating)?

ადევნება (tailgating, ასევე ცნობილია, როგორც "piggybacking") ფიზიკური შეტევის ტიპია, როდესაც არაავტორიზებული პირი, სოციალური ინჟინერიის საშუალებით, წვდომას მოიპოვებს დაცულ ტერიტორიაზე (მაგ. სადარბაზო, ოფისი, დაცული ოთახი და ა.შ). მაგალითისთვის, შემტევმა შეიძლება თავი წარმოაჩინოს როგორც მძღოლი, კურიერი, ოფისის მომსახურე სტაფი, დამლაგებელი, ელექტრიკოსი ან სხვა. შემტევი შეიძლება იცდიდეს კართან და როგორც კი თანამშრომელი/მცხოვრები კარს გა-

აღებს, თავდამსხმელი სთხოვს თანამშრომელს/მცხოვრებს კარის დაჭერას, რითაც წვდომას შენობის ტერიტორიაზე მოიპოვებს.

**რა არის დაშინება (Scareware)?**

Scareware სოციალური ინჟინერიის ერთ-ერთი სახეა, რომელიც მოიცავს მსხვერპლის დაშინებას ყალბი განგაშით და ფიქტიური მუქარით. შემტევი მსხვერპლს აშინებს, რომ მისი სისტემა დაინფიცირებულია მავნე პროგრამით, რისთვისაც ახალი პროგრამული უზრუნველყოფის დაინსტალირებას სთავაზობს. რეალურად, ზემოხსენებული პროგრამის დაინსტალირება, კრიმინალს მსხვერპლის კომპიუტერზე დისტანციური წვდომის საშუალებას აძლევს.

### 2.2.2. რა უნდა ვიცოდეთ ფიშინგის შესახებ?

ფიშინგის შეტევები შესაძლოა სხვადასხვა ტიპის ორგანიზაციებიდან მოდიოდეს, როგორიცაა საქველმოქმედო ორგანიზაციები, ტანსაცმლის მაღაზიები, სუპერმარკეტების ქსელი და ა.შ. ასევე, ხშირად, თავდამსხმელები სარგებლობენ მიმდინარე მოვლენებითა და წელიწადის გარკვეული პერიოდით. მაგალითად, ფიშინგ შეტევები შეიძლება ითვალისწინებდეს შემდეგს:

- ¬ ბუნებრივი კატასტროფები (მაგ., ქარიშხალი კატრინა, ინდონეზიის ცუნამი);
- ¬ ეპიდემიები და ჯანმრთელობის საფრთხეები (მაგ., H1N1, COVID-19);
- ¬ ეკონომიკური პრობლემები;
- ¬ მთავარი პოლიტიკური მოვლენები (არჩევნები);
- ¬ დღესასწაულები (ახალი წელი, შობა, აღდგომა და ა.შ).

### 2.2.3. როგორ ამოვიცნოთ ფიშინგი?

**საეჭვო გამგზავნის მისამართი** - გამგზავნის მისამართი შეიძლება იყოს ლეგიტიმური ბიზნესის იმიტაცია. კიბერკრიმინალები ხშირად იყენებენ ელექტრონული ფოსტის მისამართს, რომელიც ძალიან ჰგავს რეპუტაციის მქონე კომპანიის მისამართს რამდენიმე სიმბოლოს შეცვლილი ან გამოტოვებული ფორმით (მაგალითად, ნაცვლად www.microsoft.com-ისა www.microsofttt.com).

**ზოგადი მისალმებები და ხელმოწერა** - ფიშინგის ერთ-ერთი მნიშვნელოვანი ინდიკატორია_ზოგადი მისალმება, როგორიცაა „ძვირფასო მომხმარებელო“ ან „ბატონო/ქალბატონო“ და ასევე, ხელმოწერის ბლოკში საკონტაქტო ინფორმაციის ნაკლებობა. შედარებისთვის, სანდო ორგანიზაცია ჩვეულებრივ მოგმართავთ სახელით და მოგაწოდებთ მათ საკონტაქტო ინფორმაციას.

**გაყალბებული ჰიპერბმულები და ვებსაიტები** - თუ კურსორს ელექტრონული ფოსტის ტექსტის რომელიმე ბმულზე გადაატარებთ და ბმულები არ დაემთხვევა ტექსტს, რომელიც მასზე გადატარებისას ჩანს, ბმული შეიძლება იყოს ყალბი. მავნე ვებსაიტები შეიძლება გამოიყურებოდეს ლეგიტიმური საიტის იდენტურად, მაგრამ URL-ში შეიძლება გამოყენებული იქნეს დომენის სხვა ვარიაცია (მაგ., .com ნაცვლად .net). საყურადღებოა, რომ კიბერკრიმინალებს შეუძლიათ გამოიყენონ URL-ის შემოკლების სერვისი ბმულის ნამდვილი დანიშნულების დასამალად.

**მართლწერა და განლაგება** - ცუდი გრამატიკისა და წინადადების სტრუქტურა, მართლწერის შეცდომები და არათანმიმდევრული ფორმატირება არის ფიშინგის შესაძლო მცდელობის ერთ-ერთი ინდიკატორი. შედარებისთვის, რეპუტაციის მქონე ინსტიტუტებს

პერსონალი ჰყავთ გამოყოფილი, რომელიც აწარმოებს, ამოწმებსა და ასწორებს მომხმარებელთა მიმოწერას.

**საეჭვო დანართები** - მავნე პროგრამის გავრცელების ერთ-ერთი ზოგადი მექანიზმია ელექტრონული ფოსტის გამოყენება, რომელიც მომხმარებელს სთხოვს ჩამოტვირთოს და გახსნას დანართის სახით მიბმული ფაილი. შემტევმა შეიძლება შექმნას გადაუდებელი აუცილებლობის ილუზია/სცენარი, რათა დაარწმუნოს მომხმარებელი, რომ წინასწარი შემოწმების გარეშე ჩამოტვირთოს ან გახსნას დანართის სახით მიბმული ფაილი.

### 2.2.4. როგორ ავირიდოთ თავიდან ფიშინგი?

- იყავით ფრთხილი სატელეფონო ზარების, SMS-ების ან ელექტრონული ფოსტის შეტყობინებების მიმართ, რომლებიც გთხოვენ სხვადასხვა სენსიტიური ინფორმაციის გაცემას. თუ უცნობი პირი აცხადებს, რომ ლეგიტიმური ორგანიზაციის წარმომადგენელია, შეეცადეთ გადაამოწმოთ მისი ვინაობა პირდაპირ კომპანიასთან.
- არ მიაწოდოთ პერსონალური ინფორმაცია ან ინფორმაცია თქვენი ორგანიზაციის, მათ შორის მისი სტრუქტურისა თუ ქსელების შესახებ, თუ არ ხართ დარწმუნებული პიროვნების უფლებამოსილებასა და ვინაობაში.
- არ გაამჟღავნოთ პირადი ან ფინანსური ინფორმაცია ელექტრონულ ფოსტაში და არ უპასუხოთ ამ ინფორმაციის მოთხოვნას მისივე საშუალებით.
- არ გააგზავნოთ სენსიტიური ინფორმაცია ინტერნეტით, სანამ არ შეამოწმებთ ვებსაიტის უსაფრთხოებას.
    - ყურადღება მიაქციეთ ვებსაიტის Uniform Resource

Locator-ს (URL). URL-ები, რომლებიც იწყება "https"-ით, მიუთითებს იმის, რომ საიტი უსაფრთხოა, ხოლო "http" - არა.

- მოძებნეთ ე.წ. დახურული ბოქლომის ხატულა (icon) - ნიშანი, რომ თქვენი ინფორმაცია ქსელში გადაცემისას დაშიფრული იქნება.

- თუ არ ხართ დარწმუნებული, არის თუ არა ელექტრონული ფოსტით მიღებული მოთხოვნა ლეგიტიმური, შეეცადეთ გადაამოწმოთ იგი უშუალოდ კომპანიასთან დაკავშირების გზით. თუმცა არ გამოიყენოთ საკონტაქტო ინფორმაცია, რომელიც მიიღეთ ელექტრონული ფოსტის საშუალებით. ამის ნაცვლად, შეამოწმეთ კომპანიის საკონტაქტო ინფორმაცია სხვადასხვა ალტერნატიული წყაროს გზით (საძიებო სისტემები, სოციალური მედიის პოსტები და ჯგუფები და ა.შ).
- დააინსტალირეთ და გამოიყენეთ ანტივირუსული პროგრამული უზრუნველყოფა, firewall და ელექტრონული ფოსტის ფილტრები.
- ისარგებლეთ ფიშინგის საწინააღმდეგო ფუნქციით, რომელსაც გთავაზობთ თქვენი ელექტრონული ფოსტის კლიენტი და ვებ ბრაუზერი.
- გამოიყენეთ მრავალფაქტორიანი ავთენტიფიკაცია (MFA).

### რას აკეთებთ, თუ გგონიათ, რომ მსხვერპლი ხართ?

- თუ თვლით, რომ შესაძლოა გაამჟღავნეთ თქვენი ორგანიზაციის შესახებ სენსიტიური ინფორმაცია, აუცილებლად შეატყობინეთ ორგანიზაციის შესაბამის თანამშრომლებს (ინფორმაციული უსაფრთხოების დეპარტამენტი, IT დეპარტამენტი).

- თუ ფიქრობთ, რომ თქვენი საბანკო ანგარიშები შეიძლება გატეხილი იყოს, დაუყოვნებლივ დაუკავშირდით თქვენს საფინანსო ინსტიტუტს (ბანკს) და დახურეთ ნებისმიერი ანგარიში, რომლსაც საფრთხე დემუქრა. თვალყური ადევნეთ თქვენს ანგარიშზე რაიმე აუხსნელ ტრანზაქციებს.
- დაუყოვნებლივ შეცვალეთ ნებისმიერი პაროლი, რომელიც შესაძლოა ცნობილი გახდა შემტევისთვის. თუ იყენებდით ერთი და იგივე პაროლს სხვადასხვა რესურსისთვის, დარწმუნდით, რომ შეცვალეთ იგი თითოეული ანგარიშისთვის და აღარ გამოიყენოთ ეს პაროლი მომავალში.
- დაუკავშირდით პოლიციას და აცნობეთ კიბერშეტევის შესახებ.

## 2.3. დეზინფორმაცია ონლაინ სივრცეში: იდენტიფიკაცია და კონტროლის პრევენციული მექანიზმები

ევროპის საბჭოს განმარტებით, პროპაგანდას, დეზინფორმაციასა და ყალბ ამბებს აქვს პოტენციალი, ხელი შეუწყოს საზოგადოებრივი აზრის პოლარიზაციას, ძალადობრივი ექსტრემიზმსა და სიძულვილის ენას და, საბოლოოდ, ძირი გამოუთხაროს დემოკრატიებს და შეამციროს ნდობა მათ მიმართ.

ტერმინების „პროპაგანდა“, „დეზინფორმაცია“ და „ყალბი ამბები“ მნიშვნელობა ხშირად ერთმანეთს ემთხვევა. ისინი გამოიყენება სხვადასხვა გზების აღსანიშნავად, რომლითაც ინფორმაციის გაზიარება იწვევს ზიანს, განზრახ თუ უნებლიედ - ჩვეულებრივ, კონკრეტული მორალური ან პოლიტიკური მიზეზის ან თვალსაზრისის ხელშეწყობასთან დაკავშირებით.

შესაძლებელია გამოვყოთ ინფორმაციის სამი აშკარად განსხვავებული გამოყენება, რომლებიც MDM კატეგორიას მიეკუთვნება:

- Mis-information (არასწორი ინფორმაცია) - ცრუ ინფორმაცია, რომელიც გაზიარებულია ზიანის მიყენების განზრახვის გარეშე.
- Dis-information (დეზინფორმაცია) - ცრუ ინფორმაცია გაზიარებული განზრახ ზიანის მიყენების მიზნით.
- Mal-information (მავნე ინფორმაცია) - ჭეშმარიტი ინფორმაცია, რომელიც გაზიარებულია განზრახ ზიანის მიყენების მიზნით.

მიუხედავად იმისა, რომ არცერთი ეს ფენომენი არ არის უჩვეული, მათ მიიღეს ახალი მნიშვნელობა ბოლო დროს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების (ICT) დახვეწილი ფორმების ფართო ხელმისაწვდომობით. მაგალითად, ტექსტის, სურათების, ვიდეოების ან ბმულების ონლაინ გაზიარება, საშუალებას აძლევს რამდენიმე საათში ვირუსული გახდეს ინფორმაცია.

### 2.3.1. როგორ ამოვიცნოთ MDM

შეაფასეთ საინფორმაციო ლანდშაფტი კრიტიკულად და დაუთმეთ დრო წყაროებისა და შეტყობინებების გადახედვას.

შინაარსის ნახვისას, ნებისმიერი ფორმით, დაუსვით საკუთარ თავს შემდეგი კითხვები:

- იწვევს თუ არა ემოციურ რეაქციას?
- აკეთებს თუ არა გაბედულ განცხადებას საკამათო საკითხზე?
- ეს უჩვეულო პრეტენზიაა?

- შეიცავს ის clickbait-ს?
- შეიცავს თუ არა აქტუალურ ინფორმაციას, რომელიც კონტექსტში ჯდება?
- იყენებს თუ არა ის გაზვიადებულ ან დამახინჯებულ მცირე ინფორმაციას?
- გავრცელდა თუ არა ის ვირუსულად შეუმოწმებელ ან ნაკლებად გადამოწმებულ პლატფორმებზე?

ეს არის რამდენიმე სახელმძღვანელო კითხვა, რომელიც დაგეხმარებათ MDM-ის იდენტიფიცირებაში. მაშინაც კი, თუ ერთერთი შეკითხვა ეხება წყაროს, ის ავტომატურად არ ახდენს ინფორმაციის დისკრედიტაციას. ეს გახლავთ ერთგვარი, რათა უკეთ გამოიკვლიოთ საკითხი, სანამ მას ენდობით.

### 2.3.2. როგორ შეუძლიათ ორგანიზაციებს მიიღონ ზომები MDM-ის წინააღმდეგ?

ორგანიზაციებს შეუძლიათ დაიცვან თავი MDM-ის საფრთხისგან შემდეგი სტრატეგიებისა და კონტროლის გამოყენებით:

- დააყენეთ სოციალური მედიისა და ვებ მონიტორინგის სისტემა, ასევე გაფრთხილების სერვისები თქვენს ბრენდთან და ორგანიზაციებთან დაკავშირებული ყალბი ამბების იდენტიფიკაციისა და თვალყურის დევნებისთვის. ეს სერვისები ხშირად გაძლევთ საშუალებას აკონტროლოთ არა მხოლოდ თქვენი საკუთარი სოციალური მედიის პროფილები, არამედ საჯარო პოსტები, ვებ ფორუმები, ვებსაიტები, მიმოხილვები, ხსენებები და ა.შ.

- გამოიყენეთ საძიებო სისტემის ოპტიმიზაცია (SEO) გამჭვირვალე, მაღალი ხარისხის კონტენტთან ერთად ნებისმიერ ვებ გვერდზე. SEO გამოიყენება თქვენი საიტისა და სოციალური მედიის ოპტიმიზაციისთვის საძიებო სისტემებში (როგორიცაა Google) და შეუძლია განასხვავოს ვებსაიტის პოზიციის ჩვენება (ზემოთ ან ქვემოთ MDM-თან მიმართებაში, რომელიც მიზნად ისახავს თქვენს ორგანიზაციას).
- გამოიყენეთ პასუხების ძრავის ოპტიმიზაცია (AEO), რომელიც ფოკუსირებულია ხმოვან ასისტენტებზე, როგორიცაა Google Home, Amazon Alexa ან Siri ამ მოწყობილობების პასუხების ოპტიმიზაციისთვის, რათა მითითებულ იქნეს ფაქტები თქვენი ორგანიზაციის შესახებ და არა ცრუ ინფორმაცია.
- გამოიყენეთ გამაძლიერებელი ქსელები, რათა გაზარდოთ თქვენი კონტენტის წვდომა და ხილვადობა და ასევე, თავიდან აიცილოთ ცრუ ინფორმაციის გავრცელება. გამაძლიერებელი ქსელები მოქმედებს როგორც „სიმართლის დინამიკები“ და შეიძლება მოიცავდეს ორგანიზაციის პარტნიორებს, ბრენდის ელჩებსა და არსებულ მომხმარებლებს.
- წაახალისეთ ჩართულობა თქვენს კლიენტებთან და მომხმარებლებთან, რათა უზრუნველყოთ ნდობის დამყარება და შენარჩუნება. მაგალითად, საძიებო სისტემები იყენებენ მომხმარებლებისა და მათ შესახებ მიმოხილვას, რათა უკეთ შეფასდეს ბრენდის სანდოობა.
- შექმენით რეაგირების ჯგუფი, რათა ირიბად დაუპირისპირდეს ნებისმიერ MDM კამპანიას და სწრაფ დროში მომხმარებლებისთვის პასუხების გაცემა უზრუნველყოს.
- ნუ შეხვალთ პირდაპირ კომუნიკაციაში MDM-თან. პასუხები

უნდა იყოს პასიური ხასიათის და არ უნდა განთავსდეს იმ პოსტის ქვეშ, რომელშიც მოცემულია MDM. სანაცვლოდ, თქვენ შეგიძლიათ გამოაქვეყნოთ პასუხი თქვენს ვებსაიტზე. დარწმუნდით, რომ MDM-ზე პასუხი მოიცავს დეტალურ, გამჭვირვალე, ფაქტობრივ პასუხებს. საპასუხო მიდგომები შეიძლება განსხვავდებოდეს ორგანიზაციის მიხედვით.

### 2.3.3. როგორ შეუძლიათ მომხმარებლებმა მიიღონ ზომები MDM-ის წინააღმდეგ?

როგორც ინფორმაციის მომხმარებელს, შეგიძლიათ განახორციელოთ შემდეგი ქმედებები შინაარსის შემდგომ გამოსაკვლევად და MDM-ისგან თავის დასაცავად:

- მოძებნეთ უადგილო დიზაინის ელემენტები, როგორიცაა არაპროფესიონალური ლოგოები, ფერები, ინტერვალი და ანიმაციური გიფები.
- გადაამოწმეთ დომენის სახელები, რათა დარწმუნდეთ, რომ ისინი ორგანიზაციას შეესაბამება. დომენის სახელში შეიძლება იყოს შეცდომა ან გამოყენებული იყოს უმაღლესი დონის დომენი (TLD), როგორიცაა .net ან .org
- შეამოწმეთ, ორგანიზაციას აქვს თუ არა მითითებული საკონტაქტო ინფორმაცია, ფიზიკური მისამართი და გვერდი „ჩვენ შესახებ“.
- შეასრულეთ დომენის ძიება WHOIS სისტემაში, რათა ნახოთ, ვინ ფლობს ამ დომენს და შეძლოთ დადასტურება, ეკუთვნის თუ არა სანდო ორგანიზაციას. WHOIS არის დომენის სახელების მონაცემთა ბაზა და აქვს დეტალები დომენის მფლობელის შესახებ, როდის დარეგისტრირდა დომენი და

როდის იწურება ვადა.

- ¬ ჩაატარეთ გამოსახულების ძიება (reverse image search), რათა დარწმუნდეთ, რომ სურათები არ არის კოპირებული ლეგიტიმური ვებსაიტიდან ან ორგანიზაციიდან.
- ¬ გამოიყენეთ ფაქტების შემმოწმებელი საიტი, რათა დარწმუნდეთ, რომ ინფორმაცია, რომელსაც კითხულობთ, უკვე არ არის დადასტურებულად მცდარი.
- ¬ ავტომატურად არ იფიქროთ, რომ მიღებული ინფორმაცია სწორია, მაშინაც კი, თუ ის მომდინარეობს სანდო წყაროდან (როგორიცაა მეგობარი ან ოჯახის წევრი).
- ¬ დარწმუნდით, რომ ინფორმაცია არ არის მოძველებული.

## 2.4. მიწოდების ჯაჭვის კიბერუსაფრთხოება

### 2.4.1. შესავალი - რა არის მიწოდების ჯაჭვი?

ევროპის კავშირის კიბერუსაფრთხოების სააგენტოს განმარტებით (The European Union Agency for Cybersecurity – ENISA) - „მიწოდების ჯაჭვი წარმოადგენს პროცესების, ადამიანების, ორგანიზაციებისა და დისტრიბუტორების ეკოსისტემას, რომლებიც მონაწილეობენ საბოლოო გადაწყვეტის ან პროდუქტის შექმნისა და მიწოდების პროცესში. კიბერუსაფრთხოებაში მიწოდების ჯაჭვი მოიცავს რესურსების ფართო სპექტრს (ტექნიკა და პროგრამული უზრუნველყოფა) - სანახი (ღრუბლოვანი ან ლოკალური), დისტრიბუციის მექანიზმები (ვებ აპლიკაციები, ონლაინ მაღაზიები) და მართვის პროგრამული უზრუნველყოფა“.

ENISA განსაზღვრავს მიწოდების ჯაჭვის ოთხ ძირითად ელემენტს:

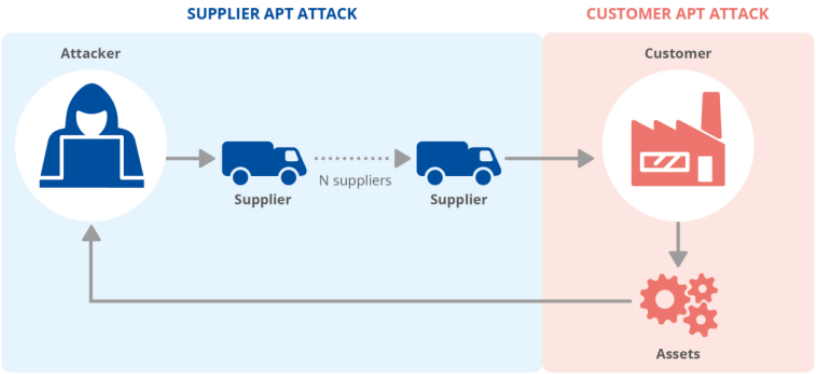
- **მიმწოდებელი:** ერთეული, რომელიც აწვდის პროდუქტს ან მომსახურებას სხვა სუბიექტს.
- **მიმწოდებლის აქტივები:** ღირებული ელემენტები, რომლებსაც მიმწოდებელი იყენებს პროდუქტის ან მომსახურების წარმოებისთვის.
- **მომხმარებელი:** სუბიექტი, რომელიც მოიხმარს მიმწოდებლის მიერ წარმოებულ პროდუქტს ან მომსახურებას.
- **მომხმარებელთა აქტივები:** ღირებული ელემენტები, რომლებიც სამიზნეს ეკუთვნის.

ერთეული შეიძლება იყოს ინდივიდი, ინდივიდთა ჯგუფი ან ორგანიზაცია. აქტივებად შეიძლება ჩაითვალონ ადამიანები, პროგრამული უზრუნველყოფა, დოკუმენტები, ფინანსები, აპარატურა ან სხვა.

### 2.4.2. როგორ იყენებენ შემტევები?

ENISA-ს განმარტებით, მიწოდების ჯაჭვის შეტევა არის მინიმუმ ორი შეტევის კომბინაცია. პირველი თავდასხმა ხდება მიმწოდებელზე, რომელიც შემდეგ აქტივების წვდომის მისაღებად სამიზნეზე თავდასხმისთვის გამოიყენება. სამიზნე შეიძლება იყოს საბოლოო მომხმარებელი ან სხვა მიმწოდებელი. ამიტომ, იმისთვის, რომ თავდასხმა კლასიფიცირდეს, როგორც მიწოდების ჯაჭვის შეტევა, მიმწოდებელი და მომხმარებელი უნდა იყოს სამიზნე.

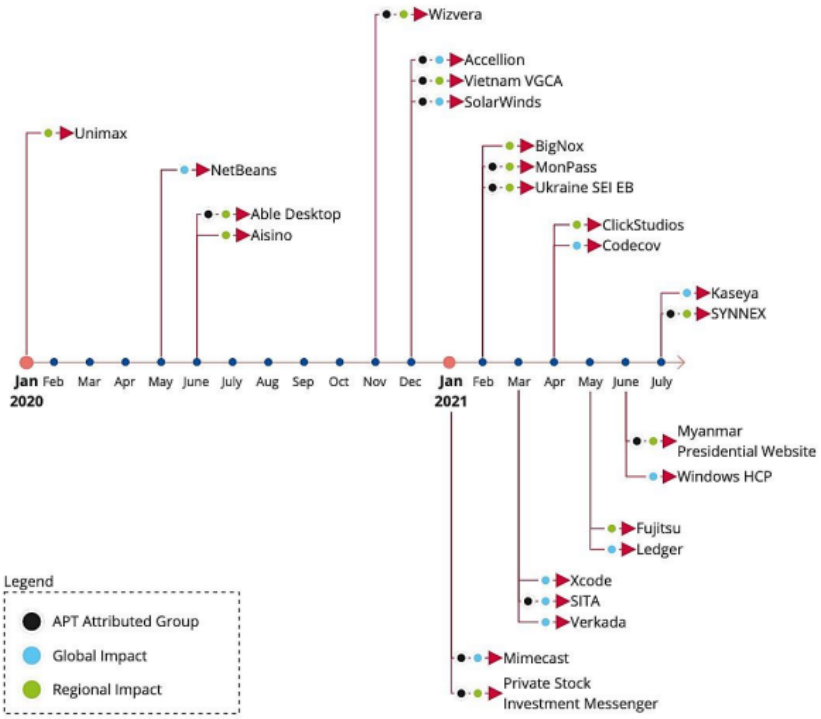
დიაგრამაზე მოყვანილია “მარტივი მექანიზმი”, თუ როგორ ხდება მიწოდების ჯაჭვის შეტევა ჰაკერული დაჯგუფების მიერ (Advanced Persistent Threat – APT). პირველ რიგში, ხდება მიმწოდებლის კომპრომიტირება, რაც შემდგომ იწვევს მომხმარებლის კომპრომიტირებას.




დიაგრამა #1: ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

### 2.4.3. რატომ არის მნიშვნელოვანი?

2020-2021 წლებში ვიხილეთ არაერთი მიწოდების ჯაჭვის შეტევა სხვადასხვა ქვეყნის სახელმწიფო თუ კერძო სტრუქტურებზე. დიაგრამა #2-ზე მოცემული სხვადასხვა შეტევის შესახებ ინფორმაციიდან საყურადღებოა ის ფაქტი, რომ შეტევების უკან ძირითადად სახელმწიფოების მიერ დაფინანსებული APT ჯგუფები დგანან და ამ შეტევებს ჰქონდა, როგორც რეგიონული, ასევე გლობალური გავლენა.

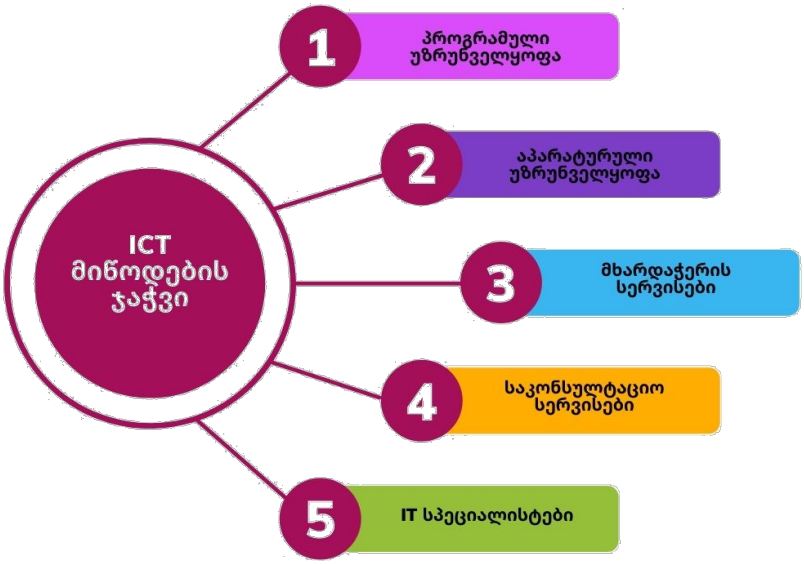



დიაგრამა #2: ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

ზემოხსენებული შეტევებიდან ერთ-ერთი ყველაზე მეტად გახმაურებული შეტევის მაგალითია SolarWinds Orion-ის შემთხვევა. აღნიშნული შეტევა მიკუთვნებული იქნა რუსეთის საგარეო დაზვერვასთან (Russian Foreign Intelligence Service (SVR)) დაკავშირებულ APT 29 დაჯგუფებასთან.

### 2.4.4. მიწოდების ჯაჭვის ტიპები

მიწოდების ჯაჭვის უსაფრთხოების საკითხი კომპლექსურია და მნიშვნელოვანია შეირჩეს სწორი მიდგომა საკითხის მიმართ. მაგალითისთვის, შეგვიძლია განვიხილოთ შემდეგი კატეგორიის მიწოდების ჯაჭვის ელემენტები:




### 2.4.5. საფრთხის შემცველი პროგრამული უზრუნველყოფის შესყიდვა

ICT მიწოდების ჯაჭვთან დაკავშირებული რისკების ერთ-ერთი პირველი მაგალითია საფრთხის შემცველი პროგრამული უზრუნველყოფის შესყიდვა / გამოყენება. კლასიკური გაგებით, პროგრამული უზრუნველყოფა:

1. შეიძლება შეიცავდეს მავნე კოდს, რომელიც აზიანებს მომხმარებელს;
2. შეიძლება აგროვებდეს მომხმარებლის შესახებ სენსიტიურ ინფორმაციას;

<u>განვიხილოთ რამდენიმე საფრთხის შემცველი პროგრამული უზრუნველყოფის ქეისი:</u>

I. **უსაფრთხოების სისტემა Kaspersky -** წლების მანძილზე, საქართველოში ერთ-ერთი ყველაზე მეტად გავრცელებული უსაფრთხოების სისტემა იყო Kaspersky-ის ანტივირუსი. როგორც კერძო, ასევე საჯარო სტრუქტურები, აქტიურად იყენებდნენ „ლეგენდარულ“ ანტივირუსს, რომელიც, როგორც ამბობდნენ, „რუსულ ვირუსებს კარგად იჭერდა“. აშშ-ის კომუნიკაციების ფედერალურმა კომისიამ (Federal Communications Commission) კასპერსკის პროდუქტები ეროვნული უშიშროების საფრთხედ მიიჩნია და აკრძალა გამოყენება. ანალოგიურად, ბრიტანეთის და გერმანიის მთავრობებმაც მოუწოდეს მომხმარებლებს ზემოხსენებული პროდუქტების გამოყენებისგან თავის შეკავებისკენ.

II. **Mail.Ru -** რუსული საფოსტო სერვისი, რომელიც აქტიურად გამოიყენება პოსტსაბჭოთა სივრცის ქვეყნებში. მნიშვნელოვანია, მომხმარებელმა გააცნობიეროს, რომ მსგავსი სერვისის გამოყენებისას მომხმარებლების პერსონალური მონაცემები, მიმოწერები, ინტერესები და ქცევა შესაძლოა გამოყენებული იქნეს რუსული სპეცსამსახურების მიერ.

III. **1C ERP –** 1C არის რუსული კომპანია, რომლის პროდუქტი 1C ERP ფართოდ არის გავრცელებული საქართველოში.

დამატებით, ადგილობრივ ბაზარზე ბევრი საკონსულტაციო კომპანიაა, რომელიც უზრუნველყოფს ამ სისტემის დეველოპმენტს და მხარდაჭერას. გადაწყვეტილების მიღებისას მნიშვნელოვანია კომპანიის ხელმძღვანელებმა გააცნობიერონ, რომ ორგანიზაციის ბიზნეს პროცესების გაციფრულებისას გამოყენებული რუსული პროგრამული უზრუნველყოფა შეიცავს შემდეგ რისკებს: მიწოდების ჯაჭვის შეტევის სიმარტივე და დამოკიდებულება რუსულ პროდუქტზე (რომელიც შესაძლოა აღარ იყოს ხელმისაწვდომი გეოპოლიტიკური ვითარებისა და სანქციების გათვალისწინებით).

IV. Yandex Taxi - ტაქსის სერვისი, რომელიც რუსულ პროგრამულ უზრუნველყოფას იყენებს და აგროვებს მომხმარებლის შესახებ სხვადასხვა სახის პერსონალურ და საბანკო მონაცემებს: სახელი, გვარი, მისამართი, ტელეფონის ნომერი, გადაადგილების მარშრუტები, საბანკო ბარათის მონაცემები და ა.შ. სხვადასხვა წყაროზე დაყრდნობით, იანდექსი აქტიურად თანამშრომლობს რუსეთის ფედერალური უსაფრთხოების სამსახურთან და აწვდის მომხმარებლების შესახებ ინფორმაციას, რასაც რუსული კანონმდებლობა კომპანიას ავალდებულებს. ინდივიდუალურ ჭრილში შესაძლოა არ იყოს კრიტიკული ერთი რომელიმე მომხმარებლის შესახებ ინფორმაცია, თუმცა, ეროვნულ დონეზე, დიდი რაოდენობით პერსონალური მონაცემების გადაცემა მტრულად განწყობილი სახელმწიფოსთვის ეროვნული უსაფრთხოების ახალ გამოწვევებს ქმნის.

<u>სია არ არის სრული და ამომწურავი.</u>

### 2.4.6. საფრთხის შემცველი აპარატურის შესყიდვა

საფრთხის შემცველი აპარატურის შესყიდვის ერთ-ერთი ყველაზე მეტად გავრცელებული მაგალითია **ჩინური წარმოების სათვალთვალო სისტემების შესყიდვა.** საერთაშორისო საუკეთესო პრაქტიკა აჩვენებს, რომ მიწოდები ჯაჭვის შეტევებში შესაძლებელია გამოყენებული იქნეს აპარატურაც (hardware). შესაბამისად, **განვითარებული** სახელმწიფოები მუშაობენ საფრთხის შემცველი აპარატურის მწარმოებლების გამოვლენასა და მათ აკრძალვაზე. მაგალითისთვის, **აშშ-ში სამთავრობო სტრუქტურებში გამოყენებისთვის/შესყიდვისთვის აკრძალულია ჩინური მწარმოებლების Huawei, Dahua, Hikvision აპარატურა** (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, https://www.acquisition.gov/far/4.2101).

### 2.4.7. მხარდაჭერის სერვისებთან დაკავშირებული რისკები

პროგრამული და აპარატურული უზრუნველყოფის მიწოდების ჯაჭვის რისკების განხილვისას, მნიშვნელოვანია სწორად იქნეს შეფასებული მხარდაჭერის სერვისის გამწევ მხარესთან დაკავშირებული რისკებიც. კერძოდ, ნებისმიერი პროგრამული თუ აპარატურული უზრუნველყოფის შესყიდვა ითვალისწინებს თანმხლებ საგარანტიო პირობებსა და შესაბამის მხარდაჭერის სერვისებს. პროექტის საწყის ეტაპზე ხდება საჭიროებების განსაზღვრა, ლიცენზიების მოცულობისა თუ აპარატურული გადაწყვეტის შერჩევა, შეფასება და ინტეგრაცია, რასაც შემდგომში მოყვება სხვადასხვა ტიპის მხარდაჭერის სერვისი (მაგალითად, ა) 5 ბიზნეს დღე, 9 სამუშაო საათი; ბ) 7 დღე, 24 საათი და ა.შ).

მნიშვნელოვანია გაითვალისწინოთ მხარდამჭერი სერვისის მიმწოდებელი კომპანიის რეგიონი და უზრუნველყოთ თანამშრომლობა მეგობრული ან ნეიტრალური სახელმწიფოს ოფისის წარმომადგენლებთან.

### 2.4.8. საკონსულტაციო სერვისების მიწოდებასთან დაკავშირებული საფრთხეები

მსგავსად პროგრამული უზრუნველყოფისა და აპარატურის შესყიდვისა, მნიშვნელოვანია **სერვისის მიწოდების ჯაჭვის საფრთხეების მართვაც**. საკონსულტაციო სერვისებთან დაკავშირებული რისკებია:

კონსულტანტების შერჩევისას, მნიშვნელოვანია გათვალისწინებული იქნეს მათი წარმომავლობა და პროფესიული უნარები. საკონსულტაციო სერვისის გაწევისას, კონსულტანტები აგროვებენ ინფორმაციას ორგანიზაციის ინფრასტრუქტურის შესახებ, სწავლობენ სისუსტეებსა და ძლიერ მხარეებს, აკვირდებიან თანამშრომლების უნარებს და მზაობას, იმოქმედონ კრიტიკულ ვითარებაში. მნიშვნელოვანია, ორგანიზაციამ გაიაზროს ზემოხსენებული რისკები და უზრუნველყოს ორგანიზაციის შესახებ კრიტიკული ინფორმაციის გადაცემის მაქსიმალური შეზღუდვა მტრულად განწყობილი ქვეყნების წარმომადგენლებისთვის. ასეთი საკონსულტაციო სერვისების მაგალითებია: ფინანსური აუდიტი, შესაბამისობის აუდიტი, IT აუდიტი, ორგანიზაციული აუდიტი, ინფორმაციული უსაფრთხოების აუდიტი და საკონსულტაციო მომსახურება, IT შეფასება, IT ინფრასტრუქტურული პროექტები და სხვა.

### 2.4.9. IT კადრების მიგრაცია

რუსეთის ფედერაციის მიმართ დაწესებული სანქციების პარალელურად, ბევრი რუსი IT სპეციალისტი საქართველოში საცხოვრებლად გადმოვიდა, რათა თავიდან აიცილონ სანქციები და განაგრძონ მუშაობა ევროპულ და საერთაშორისო პროექტებ-

ზე. საქართველოს აქვს საკმაოდ კარგი საგადასახადო კანონმდებლობა პროგრამული უზრუნველყოფის შემქმნელებისა და პროგრამული უზრუნველყოფის მწარმოებლების მოსაზიდად (საშემოსავლო გადასახადი 5 პროცენტამდე).

ამჟამინდელი მდგომარეობით, შეუძლებელია ზუსტად შეფასდეს ზემოთ აღნიშნული მიგრაციის პოტენციური შედეგები. დამატებით კვალიფიციური კადრების შემოდინებამ შეიძლება ხელი შეუწყოს საჯარო და კერძო კომპანიების ციფრულ ტრანსფორმაციას, რადგან საქართველოს აქვს კვალიფიციური IT პერსონალის დეფიციტი. ადგილობრივ კომპანიებს, მათ შორის, ქვეყნის კრიტიკულ ინფორმაციულ ინფრასტრუქტურას, საშუალება აქვთ არსებული დეფიციტი ბაზარზე ახლადგაჩენილი კვალიფიციური მიგრანტებითა და მათი კომპანიებით შეივსონ მაშინ, როცა პრაქტიკაში არსებობს ძალიან ცოტა ეფექტური კონტროლის მექანიზმი რისკების კომპენსაციისთვის.

მეორე მხრივ, <u>დაჩქარებული ციფრული ტრანსფორმაციის ფასი შეიძლება იყოს კომპრომეტირებული კრიტიკული ინფორმაციული ინფრასტრუქტურა.</u> რუსეთთან რეგიონული ურთიერთობების კონტექსტის გათვალისწინებით, საქართველოს ემუქრება მომეტებული საფრთხეები, რომლებიც დაკავშირებულია მიწოდების ჯაჭვთან და ე.წ. ინსაიდერ საფრთხეებთან (insider threat). <u>კლასიკური განმარტებით, ზემოხსენებული ახლადშექმნილი კომპანიები არ ჯდებიან მიწოდების ჯაჭვის შეტევე-</u>

ბის განმარტებაში, მაგრამ რუსეთის სპეცსამსახურები, როგორც წესი, ითხოვენ პირდაპირ ან ირიბ წვდომას მომხმარებლის მონაცემებზე რუსული კომპანიებისგან, რაც წარმოქმნის როგორც მიწოდების ჯაჭვის, ასევე ინსაიდერის საფრთხეებს. გარდა ამისა, საქართველოს საჯარო სექტორს ექნება მცირე ან საერთოდ არ ექნება იურიდიული ბერკეტი, რათა საკუთარი ტენდერებიდან ადგილობრივად რეგისტრირებული IT კომპანიები გაფილტროს.

## 2.5. სოციალური ქსელის უსაფრთხო გამოყენება

სოციალური ქსელები ბოლო ათწლეულის განმავლობაში განსაკუთარებული პოპულარობით სარგებლოს. ეს არის მუდმივი კავშირის დამყარების შესანიშნავი შესაძლებლობა საკუთარ მეგობრებთან, ოჯახის წევრებთან თუ სრულიად უცნობ ადამიანებთან. მისი საშუალებით თანამედროვე ადამიანი იღებს ზღვა ინფორმაციას, სპეციფიკური ინტერესებისა და სანაცნობო წრის მიხედვით. მილიონობით ადამიანი სხვადასხვა სოციალურ ქსელს ყოველდღიურად იყენებს, მათი საერთო რაოდენობა კი რამდენიმე მილიარდს აღწევს. მათ შორის, განსაკუთრებული პოპულარობით სარგებლობს ისეთი სოციალური ქსელები, როგორებიცაა: Facebook, TikTok, Instagram, WeChat, PinTerest, Linkedin და ა.შ. უამრავ ცნობილ ორგანიზაციასა თუ პიროვნებას აქვს შექმნილი სოციალური ქსელის ანგარიში და იყენებს მას, როგორც ფართო აუდიტორიასთან კავშირისა და კომუნიკაციის საშუალებას.

გთავაზობთ 10 რჩევას, რაც უნდა გაითვალისწინოთ სოციალური ქსელებით უსაფრთხოდ სარგებლობისთვის:

### 2.5.1. შეამოწმეთ პარამეტრები

სოციალური ქსელის გამოყენება იწყება მასზე დარეგისტრი-

რებით, ე.წ. ანგარიშის შექმნით. უკვე ამ ეტაპზე ნაბიჯ-ნაბიჯ შეხვდებით შეტყობინებებსა და რეკომენდაციებს თუ რისი გაკეთებაა მიზანშეწონილი რეგისტრაციისას. მაგალითად: მარტივად დასამახსოვრებელი პაროლის შეყვანისას, სოც-ქსელი ავტომატურად გირჩევთ, რომ დააყენოთ რთული პაროლი, ასევე ერთ-ერთ ვარიანტად შემოგთავაზებთ დამატებით უსაფრთხოების ზომასაც, როგორიცაა მობილურზე ერთჯერადი კოდის მიღებით აუტენტიფიკაციის გავლა - ნუ უგულებელყოფთ ამ შემოთავაზებებს და გაითვალისწინეთ უსაფრთხოების მოთხოვნები საწყის ეტაპებზეც.

მას შემდეგ, რაც დარეგისტრირდებით, კარგი იქნება თუ მიაკითხავთ მენიუში განთავსებულ უსაფრთხოებისა და პრივატულობის განყოფილებებს. აქ დაგხვდებათ ყველა ის მნიშვნელოვანი პარამეტრი, რისი გამართვითაც საგრძნობლად შეამცირებთ ისეთი სამომავლო ინციდენტების ალბათობას, როგორებიცაა:

- თქვენი ექაუნთის ე.წ. გატეხვა/დაჰაკვა, ანუ მასზე არასანქცირებული წვდომა;
- თქვენ მიერ მართული გვერდების დაკარგვა;
- თქვენი პირადი მიმოწერის სხვის ხელში ჩაგდება/გასაჯაროება;
- არასასურველი პიროვნებებისგან შემაწუხებელი წერილებისა და პოტენციურად საფრთხის შემცველი ლინკების მიღება და ა.შ.

გახსოვდეთ, უსაფრთხოების პარამეტრების დაყენებისას დახარჯული რამოდენიმე წუთი, სამომავლოდ მნიშვნელოვნად დაგიზოგავთ დროსა და ნერვებს, დიდი ალბათობით აგარიდებთ

თავიდან უსიამოვნო ინციდენტებსა და შეამცირებს კიბერ-უსაფრთხოების რისკებს.

### 2.5.2. იცნობდეთ და მართეთ თქვენი სამეგობრო წრე

მას შემდეგ, რაც სოც. ქსელზე დარეგისტრირდებით, როგორც წესი, პირველი ნაბიჯია ნაცნობ-მეგობრებისა და საინტერესო პიროვნებების ე.წ. „მეგობრებად“ დამატება, მათი გვერდების „გა-ყოლა/Following” და მათთან მიმოწერის დაწყება.

იყავით ყურადღებით და გადაამოწმეთ, თუ ვის იმატებთ მეგობართა წრეში. კიბერ-კრიმინალები ხშირად ქმნიან ყალბ ანგარიშებს  და ცდილობენ ამ სახით თქვენს პერსონალურ მონაცემებზე წვდომის მოპოვებას ან თაღლითობის გზით თანხის გამოძალვას.

ასევე, არ დაგავიწყდეთ, რომ მას შემდეგ, რაც დაიმატებთ ამა თუ იმ პერსონას „მეგობრებში“, მას ექნება საშუალება დაინახოს ის ფოტო, ვიდეო თუ ტექსტური მასალა, რასაც თქვენ საჯაროდ არ დებთ და მხოლოდ მეგობართა წრისთვის განკუთვნილად მოიაზრებთ.

მეორე მხრივ, მნიშვნელოვანია დააკვირდეთ რომელ გვერდებს იწონებთ და მიჰყვებით, იქნება ეს ორგანიზაცია, კომპანია თუ რომელიმე ცნობილი პიროვნება. ამ შემთხვევებშიც ხშირად იქმნება ყალბი და მიმსგავსებული გვერდები, რომლებიც ხშირად დეზინფორმაციასა და შეცდომაში-შემყვან კონტენტს (შინაარსს) ავრცელებენ.

### 2.5.3. ერთხელ დაპოსტვა, მუდმივად დაპოსტვაა - რას აზიარებთ?

გაუფრთხილდით თქვენს რეპუტაციას, იცოდეთ რომ სოციალურ ქსელში ერთხელ დადებული „დაპოსტილი“ ინფორმაცია, შეიძლება მუდმივად იქ დარჩეს, მაშინაც კი, თუ მას დადებიდან

2 წუთში აიღებთ ან წაშლით. კარგად დაფიქრდით სანამ რაიმე სახის მოწოდებას გააკეთებთ, ფოტო ან ვიდეო მასალას გაავრცელებთ. იფიქრეთ მოსალოდნელ შედეგებზე. რა შეიძლება მოჰყვეს ამას. ხშირ შემთხვევაში ადამიანებს სხვადასხვანაირი ინტერპრეტაციის მიცემა შეუძლიათ ერთი და იმავე მოვლენისთვის, შესაბამისად, უწყინარი კომენტარი, აზრი ან ფოტო/ვიდეო, შეიძლება ადამიანთა განსხვავებულმა ჯგუფმა სულ სხვანაირად გაიგოს.

რამდენიმე კვლევა ჩატარდა სოც. ქსელის გავლენასთან დაკავშირებით, რომელმაც აჩვენა, რომ, მაგალითად, გამოკითხულ დამსაქმებელთა 70%-ზე მეტს, სამსახურში ასაყვან კანდიდატებზე უარი უთქვამთ, მათ მიერ ადრე სოც. ქსელში გამოქვეყნებული ინფორმაციის გამო.

ასევე, ხშირია უსიამოვნებები, კონფლიქტები, თვეებისა თუ წლების შემდეგ უხერხული მდგომარეობები, სოციალურ ქსელში დროის გარკვეულ მონაკვეთში განხორციელებული აქტივობის გამო.

### 2.5.4. ყურადღებით იყავით ვის უზიარებთ

გასათვალისწინებელია, რომ ზემოთ ჩამოთვლილი რისკების შემცირება გარკვეულწილად შეიძლება იმ მექანიზმებით, რაც სოციალურ ქსელთა უმეტესობას ჩაშენებული აქვს, იგულისხმება - სამიზნე აუდიტორიის შეზღუდვა, კერძოდ, თქვენ შეგიძლიათ განსაზღვროთ თუ ვის შეუძლია:

- ¬ ნახოს თქვენი კონკრეტული პოსტი, ფოტო ან ვიდეო;
- ¬ მასზე კომენტარის გაკეთება;
- ¬ თქვენთვის შიდა მესიჯის მოწერა და ა.შ.

ასევე, შეგიძლიათ განსაზღვროთ ნებისმიერი თქვენი პოსტი, საჯაროა, მხოლოდ მეგობრებისთვისაა, მეგობართა მხოლოდ მცირე წრისთვისაა, თუ ჯერ მხოლოდ თქვენთვის აქვეყნებთ დამახსოვრების და სამომავლოდ დაპოსტვის მიზნით.

### 2.5.5. იცოდეთ, როგორ მოიქცეთ განსაკუთრებულ შემთხვევებში

არსებობს წინასწარ დადგენილი გზები, თუ როგორ უნდა მოიქცეთ განსაკუთრებულ შემთხვევებში. მაგალითად, თუ ვინმე თქვენ მიმართ ახორციელებს ბულინგს, დამცირებას, შანტაჟს და ა.შ. შეგიძლიათ მიწეროთ სოციალურ ქსელს შესაბამისი შეტყობინებით და დაარეპორტოთ - ანუ მიმართოთ ადმინისტრაციას, გამოიკვლიოს აღნიშული შემთხვევები და მიიღოს ზომები კონკრეტული ანგარიშის მიმართ.

მიუხედავად იმისა, რომ ხშირია ყალბი ანგარიშებით ზემოთ ჩამოთვლილი ქმედებების განხორციელება, მნიშვნელოვანია მოიქცეთ ისე, როგორც ამას კონკრეტული სოციალური ქსელის წესები მოითხოვს. ყველაზე მარტივ შემთხვევაში კი უბრალოდ წაშალეთ ან დაბლოკეთ „შემომტევი“ ანგარიშები.

ასევე, წინასწარ გაეცანით იმ გზებსა და ქმედებებს, რაც უნდა გააკეთოთ, სოციალურ ქსელზე წვდომის დაკარგვის შემთხვევაში. იცოდეთ თუ როგორ იქცევით მაშინ, თუ კიბერკრიმინალები თქვენს ექაუნთს გატეხავენ და მასზე წვდომას დაკარგავთ. გაეცანით წესებსა და პირობებს. წინასწარ გაამზადეთ ის დოკუმენტაცია ან ინფორმაცია, რასაც თქვენგან სოციალური ქსელის ადმინისტრაცია ან სამართალდამცავები მოითხოვენ.

**არსებობს რამდენიმე ტექნიკური რჩევა, რისი გათვალისწინებაც საგრძნობლად შეამცირებს თქვენს სოციალურ ქსელზე არასანქცირებული წვდომის ალბათობას, შესაბამისად, მცირ-**

დება რისკი, რომ ჰაკერებისა და კიბერკრიმინალების მსხვერპლი გახდეთ.

### 2.5.6. გამოიყენეთ რთული პაროლები

აუცილებლად გამოიყენეთ რთული პაროლები. არ გამოიყენოთ მსგავსი პაროლები სხვადასხვა საიტზე, ვინაიდან თუ სხვაგან გატეხავენ თქვენს ექაუნთს და გაიგებენ პაროლს, იგივე პაროლით შეეძლებათ თქვენს ანგარიშზე წვდომა სოციალურ ქსელშიც. ეცადეთ ყველა სოციალურ ქსელზე უნიკალური პაროლი გქონდეთ.

### 2.5.7. ჩართეთ მულტიფაქტორული აუტენტიფიკაცია

განსაკუთრებით მნიშვნელოვანია დამატებითი აუტენტიფიკაციის ჩართვა, რაც პაროლთან ერთად კიდევ ერთი იდენტიფიცირების ფაქტორის შემოღებას გულისხმობს. ძირითადად, ეს არის თქვენს მობილურ ნომერზე ერთჯერადად მოსული კოდი ან უკეთეს შემთხვევაში ერთჯერადი კოდების გენერირების აპლიკაცია.

საუკეთესო შემთხვევაში კი შეგიძლიათ შეიძინოთ ე.წ. Hardware Token (მაგალითად Yubico USB/NFC/Lightning), რომლის ფიზიკურად ფლობაც აუცილებელია რომელიმე სოციალურ ქსელსა თუ სხვა სერვისზე აუტენტიფიკაციის გასავლელად. იმ შემთხვევაშიც კი, თუ ვინმე თქვენს პაროლს მოიპოვებს, ასევე ერთჯერად SMS კოდს, მას თქვენს ანგარიშზე შესვლა მაინც არ შეეძლება. ეს უკანასკნელი მეთოდი მოითხოვს გარკვეულ ცოდნასა და უნარებს, რისი მიღებაც მწარმოებლის ვებგვერდზე და შესაბამის ინსტრუქციებშია შესაძლებელი.

### 2.5.8. დაფიქრდით სანამ დააკლიკებთ

სოციალურ ქსელებში (Post, Tweet, Messages) არსებული ლინკები კიბერკრიმინალებისთვის ადვილი გზაა თქვენს შეცდომაში შესაყვანად და სენსიტიური ინფორმაციის მოსაპოვებლად.

ყურადღებით იყავით სანამ რაიმე ლინკს დააკლიკებთ და მასზე გადახვალთ, გამოიჩინეთ განსაკუთრებული სიფრთხილე ამ ლინკებიდან რაიმეს გადმოწერის შემთხვევაში.

თუ ლინკზე გადასვლისას მოითხოვება შეიყვანოთ იმ სოციალური ქსელის ანგარიშის სახელი და პაროლი, რითაც შესული ხართ, იცოდეთ რომ ძალიან დიდი ალბათობაა ეს კიბერკრიმინალების დაგებული მახე იყოს თქვენი ექაუნთის გასატეხად.

### 2.5.9. გადაამოწმეთ წყაროები

სოციალური ქსელებიდან მიღებული ინფორმაცია მნიშვნელოვან გავლენას ახდენს ჩვენს ყოველდღურობასა და ზოგ შემთხვევაში ფაქტების აღქმაზეც. ბოლო დროს მას აქტიურად იყენებენ:

- საზოგადოებრივი აზრის ფორმირებისათვის,
- არჩევნებში ჩარევისას,
- განწყობების შესასწავლად თუ ფორმირებისათვის,
- მარკეტინგული აქტივობების დასაგეგმად,
- სპეცსამსახურების ამოცანების შესასრულებლად და ა.შ.

წესად და ჩვევად გაიხადეთ, ამა თუ ინფორმაციის მიღებისას, გადაამოწმოთ მისი წყარო. შეძლებისდაგვარად გადაამოწმეთ და გაარკვიეთ ვინ, როდის, რატომ და რა ფორმით ავრცელებს შესაბამის ინფორმაციას.

იყავით დაკვირვებულები სანამ დასკვნებს გამოიტანთ და ინფორმაციას სანდოდ ჩათვლით!

### 2.5.10. გაეცანით უსაფრთხოებისა და პრივატულობის რეკომენდაციებს

მიუხედავად აქ მოყვანილი ზოგადი რჩევებისა, არსებობს სხვადასხვა სოციალურ ქსელზე მორგებული უსაფრთხოებისა და

პრივატულობის კონკრეტული რეკომენდაციები. ხშირ შემთხვევაში, ეს ყველაფერი ჩაშენებულია იმავე სოციალურ პლატფორმაზე და ატარებს მარტივად აღსაქმელი ვიზუალური რჩევისა და განმარტების ხასიათს.

ასევე, იქმნება ბევრი ვიდეო-სახელმძღვანელო, სტატია და ბლოგი სოციალური ქსელის უსაფრთხოდ გამოყენებასთან დაკავშირებით.

სოციალური ქსელები ყოველდღიურად ნახლდება, იცვლება და ხშირად ახალი ტიპის ვებგვერდები იქმნება. ეცადეთ, არ ჩამორჩეთ უახლეს რჩევებსა და რეკომენდაციებს მათი უსაფრთხოდ გამოყენებასთან დაკავშირებით. იყავით კიბერკრიმინალებზე ერთი ნაბიჯით წინ.

## 2.6. მობილური მოწყობილობების საფრთხეები და თავდაცვის გზები

თქვენი სმარტფონი ან ტაბლეტი - ინახავს ძვირფას ინფორმაციას პირადად თქვენი, თქვენი ოჯახის, მეგობრებისა და თანამშრომლების შესახებ.

დაფიქრებულხართ, რა ინფორმაციას ჩაიგდებს ხელთ სხვა ადამიანი, იმ შემთხვევაში, თუ დაისაკუთრებს თქვენს მობილურ მოწყობილობას:

- თქვენს პირად გეგმებსა და ჩანაწერებს (Notes);
- საკონტაქტო ინფორმაციას თქვენი ნაცნობ-მეგობრების შესახებ;
- სენსიტიურ ფოტოებსა და ვიდეოებს;
- ვის და როდის ურეკავთ, გირეკავენ, რა ხანგრძლივობით;
- კონფიდენციალურ სამსახურეობრივ ფაილებს;

- არასაჯარო და მაკომპრომეტირებელ მიმოწერებს (მესენჯერები, სოც. ქსელები);
- პაროლებს სხვადასხვა საიტებისთვის და სერვისებისთვის;
- რა შინაარსის საიტებზე შედიხართ და რას ათვალიერებთ;
- ინფორმაციას ფინანსური და საბანკო შემოსავლების შესახებ;
- თქვენი წინა ადგილმდებარეობების შესახებ ცნობებს (სად ცხოვრობთ, მუშაობთ და რა ადგილებს სტუმრობთ);
- ინფორმაციას თქვენი ჯანმრთელობის შესახებ (დაავადებები, აცრები, ფიტნესი, ემოციური და რეპროქუციული ჯანმრთელობა, სირბილის მარშუტები, ალერგია, მიღებული წამლების ტიპი და ინტენსივობა) და ა.შ.

გინახავთ ალბათ სასოწარკვეთილ მდგომარეობაში მყოფი ადამიანები, რომლებმაც თავისი მობილური მოწყობილობა დაკარგეს. ამ ნერვიულობის მიზეზი კი ის პოტენციური ზიანია, რაც ტელეფონში არსებული ინფორმაციის არასანქცირებულ ხელში მოხვედრამ შეიძლება გამოიწვიოს. ამ შემთხვევაში, ზიანი გაცილებით დიდია, ვიდრე ის ფულადი დანაკარგი, რასაც ამ მოწყობილობის შეძენის ღირებულება წარმოადგენს.

გაითვალისწინეთ ქვემოთ მოცემული რჩევები, რათა შეამციროთ მობილური მოწყობილობების შესაბამისი კიბერუსაფრთხოების რისკები, დაიცვათ საკუთარი თავი, ახლობლები და საქმიანობა.

### 2.6.1. პინი, პაროლი, ანაბეჭდი და სახე

თქვენს მოწყობილობაზე დასაშვებად გამოიყენეთ რთული პინკოდები და პაროლები. თუ მოწყობილობა საშუალებას გაძლევთ, დამატებით დააყენეთ თითის ანაბეჭდი ან სახით იდენტიფიცირება. ეს გზა პირველი დაცვის ხაზია, თქვენი მოწყობილობის დაკარგვის შემთხვევაში.

მნიშვნელოვანია, რომ პინი ან პაროლი რთული იყოს (არა-1234 ან დაბადების წელი, მეტსახელი), მათი რამდენჯერმე არასწორად შეყვანის შემდეგ კი, მობილური მოწყობილობა გარკვეული დროით იბლოკებოდეს ან თქვენ შეტყობინებას გიგზავნიდეთ ადგილმდებარეობის შესახებ.

### 2.6.2. განახლებები და კიდევ ერთხელ განახლებები

იმისათვის, რომ თქვენი მობილური მოწყობილობის ოპერაციული სისტემა და მასზე არსებული აპლიკაციები მუდმივად განახლებული იყოს, გააქტიურეთ ავტომატური განახლებების ფუნქცია. ჰაკერები მუდმივად პროგრამული უზრუნველყოფის ახალი სისუსტეების ძიებაში არიან. მწარმოებლები კი თავის მხრივ უშვებენ შესაბამის განახლებებს იმისათვის, რათა აღნიშნულ გამოწვევებს გაუმკლავდნენ. მუდმივად განახლებული ოპერაციული სისტემები და აპლიკაციები მნიშვნელოვნად ართულებს თქვენი მობილური მოწყობილობის დაჰაკვას.

თუ აპლიკაციების განახლება რამდენიმე წამში სრულდება, როგორც წესი, ოპერაციული სისტემის (iOS, Android, Windows) განახლებები გარკვეულ დროს მოითხოვს (10-20 წთ), რის განმავლობაშიც მობილური მოწყობილობის გამოყენება დროებით შეუძლებელია. არ გადადოთ მნიშვნელოვანი განახლებები და არ შეცვალოთ მასთან დაკავშირებული უსაფრთხოების პარამეტრები.

### 2.6.3. თვალყურის დევნება

გადმოწერეთ და დააყენეთ ან გამართეთ სპეციალური აპლიკაცია იმისათვის, რომ თვალყური ადევნოთ თქვენს მობილურ მოწყობილობას ინტერნეტით. ამ გზით თქვენ შეძლებთ მობილური მოწყობილობის ადგილმდებარეობის დადგენას მისი დაკარგვის ან მოპარვის შემდეგ, უარეს შემთხვევაში კი შეგეძლებათ წაშალოთ მასზე არსებული ნებისმიერი ტიპის ინფორმაცია.

### 2.6.4. სანდო აპლიკაციები

გადმოწერეთ აპლიკაციები მხოლოდ სანდო და ოფიციალური პლატფორმებიდან:

- iPad და iPhone-ისათვის ეს ნიშნავს აპლიკაციების გადმოწერას ოფიციალური Apple App Store-დან;
- ანდროიდის აპლიკაციები უნდა გადმოწეროთ Google Play-დან;
- Amazon ტაბლეტისთვის კი Amazon App Store-დან და ა.შ.
- მწარმოებლის მიერ მითითებული სანდო რესურსებიდან.

როდესაც თქვენ იწერთ აპლიკაციებს უცხო და ნაკლებად ცნობილი საიტებიდან, დიდი ალბათობით ისინი არ გადის შემოწმებას და დაინფიცირებულია.

ასევე, სანამ გადმოწერთ აპლიკაციას, შეამოწმეთ, რომ მას აქვს პოზიტიური შეფასებები მომხმარებლებისგან და აქტიური განახლებები მწარმოებლისაგან.

მოერიდეთ უცნობ აპლიკაციებს, რომელთაც აქვთ ცოტა შეფასება და იშვიათად გადის განახლების პროცესს.

და ბოლოს, მიუხედავად იმისა, თუ საიდან გადმოწერეთ აპლიკაცია, რეკომენდაციას გაძლევთ წაშალოთ ის, თუ აღარ გჭირდებათ ან აქტიურად არ იყენებთ.

### 2.6.5. პრივატულობა

როდესაც აყენებთ ახალ აპლიკაციას, დარწმუნდით, რომ შეამოწმეთ მისი პრივატულობის ოფციები. მაგალითად:

- ნამდვილად სჭირდება თუ არა აპლიკაციას წვდომა ყველა თქვენი მეგობრის საკონტაქტო ინფორმაციაზე.

- ასევე გირჩევთ გააუქმოთ ადგილმდებარეობის დადგენის სერვისი ყველა იმ აპლიკაციისათვის, რომელსაც თვლით, რომ ფუნქციონირებისათვის არ სჭირდება თქვენი ადგილმდებარეობის განსაზღვრა.
- თუ თქვენ არ გაკმაყოფილებთ აპლიკაციის სხვადასხვა ნებართვა თქვენი მოწყობილობის მიმართ, გამოიყენეთ სხვა ანალოგი, რომელიც თქვენთვის მისაღები იქნება.
- ასევე, პერიოდულად შეამოწმეთ თუ რა ფუნქციებზე აქვს ნებართვა აპლიკაციას და დარწმუნდით, რომ ისინი არ შეცვლილა.

იცოდეთ, რომ აპლიკაციების მართვის სადავეები თქვენს ხელთაა და შეგიძლიათ გადაწყვიტოთ, თუ რომელ მათგანს ექნება წვდომა თქვენს **ფოტოებზე, მიმოწერაზე, ვიდეოკამერაზე, მიკროფონსა თუ ადგილმდეობარეობაზე.**

### 2.6.6. სარეზერვო ასლები

ყოველთვის გააკეთეთ თქვენი მონაცემების სარეზერვო ასლები. მობილური მოწყობილობების შემთხვევაში, შესაძლებელია სარეზერვო ასლების ან ლეპტოპებზე და პერსონალურ მოწყობილობებზე გადატანა ე.წ. backup, ან ჩაშენებული ონლაინ რეზერვირების გამოყენება (მაგალითად, icloud-ის ან google drive-ის გამოყენება). ამ შემთხვევაში, თქვენი ინფორმაცია შენახული იქნება მაშინაც კი, თუ იგი წაგეშლებათ, მოწყობილობას დაკარგავთ ან ფიზიკურად დააზიანებთ.

შედარებით მარტივია ავტომატური სარეზერვო ასლების წარმოების განხორციელება, თუმცა კარგად გაეცანით სარეზერვო ასლების წარმოების ტექნიკურ წესებს.

თავის დასაზღვევად, რამდენჯერმე სცადეთ სარეზერვო ასლების აღდგენა და დარწმუნდით, რომ ისინი ინახება (რეზერვაციას განიცდის) იმ წესის შესაბამისად, რომელიც თქვენთვის მისაღებია:

- პერიოდულობა
- მოცულობა
- სიხშირე
- სარეზერვო ფაილების შინაარსი
- შენახვის ადგილი
- შენახვის ფორმა
- და ა.შ.

### 2.6.7. სამსახური და დისტანციურად მუშაობა

სამუშაო ადგილზე ყოფნისას, გამოიჩინეთ განსაკუთრებული სიფრთხილე, რათა ვიდეო და ფოტო გადაღების შემთხვევით არ გადაიღოთ სენსიტიური ინფორმაციის მქონე ფოტო-სურათი (რომელზეც ჩანს დაფები, კომპიუტერის ეკრანები და სხვა).

ბოლო პერიოდში, პანდემიის და სხვა საფრთხეების შედეგად, ხშირად გვიწევს მობილური მოწყობილობებიდან მუშაობა, მსოფლიოს სხვადასხვა წერტილიდან - იქნება ეს სახლი, კაფე, სასტუმრო თუ ტრანსპორტი. ამ შემთხვევაში, განსაკუთრებით მომატებულია თქვენს მობილურ მოწყობილობებზე შეტევის ალბათობა, რადგან კიბერკრიმინალები აცნობიერებენ რომ თქვენი დაცვის დონე გაცილებით დაბალი იქნება, ვიდრე ეს სამსახურში (ოფისში) ყოფნისას კორპორაციულ-ორგანიზაციულ დონეზე ხდება.

გახსოვდეთ, რომ თუ დასაქმებული ხართ და მუშაობთ მობილურად/დისტანციურად, თქვენს მობილურ მოწყობილობაზე მოპოვებული არასანქცირებული წვდომა საფრთხეს უქმნის არა მხოლოდ თქვენს პერსონალურ მონაცემებს, არამედ იმ ორგანიზაციის სენსიტიურ ინფორმაციასაც, სადაც მუშაობთ. მისი დაკარგვის/გაუონვის შემთხვევაში კი შეიძლება თქვენ მიმართ დისციპლინარულ-ადმინისტრაციული ზომებიც კი გატარდეს და შესაბამისი პასუხისმგებლობა დაგეკისროთ.

### 2.6.8. გაჩუქება, გაყიდვა, გადაგდება

თუ გადაწყვეტთ შეცვალოთ თქვენი მობილური მოწყობილობა, კარგად დაფიქრდით სანამ ძველს ვინმეს გადასცემდეთ. გახსოვდეთ, რა ინფორმაციას შეიცავს ის. სრულად (და არა მხოლოდ ფოტოები) წაშალეთ თქვენი მობილური მოწყობილობა, გამოიყენეთ ე.წ. Factory Reset, Format ფუნქციები, რაც უზრუნველყოფს მასში არსებული ყველა სახის ინფორმაციის სრულად წაშლას და ქარხნულ მდგომარეობაზე დაბრუნებას.

ამ შემთხვევაში გაცილებით მცირეა იმის ალბათობა, რომ ახალმა მფლობელმა თქვენს ძველ ფაილებზე რაიმე სახის წვდომა მოიპოვოს.

### 2.6.9. WiFi ინტერნეტის გამოყენება

მობილური მოწყობილობის უპირატესობა მართლაც მისი მობილურობაა, რაც გულისხმობს ნებისმიერი ადგილიდან მუშაობას ინტერნეტ ქსელში ფიზიკურად კაბელებით ჩართვის გარეშე.

ამ შემთხვევაში, მიმზიდველი ცდუნებაა, კაფეებსა თუ საერთო სივრცეებში არსებული უფასო და ღია Wi-Fi ქსელების გამოყენება.

გახსოვდეთ, რომ ასეთი ქსელები ნაკლებად დაცულია და, ხშირ შემთხვევაში, მათი გამოყენებით განხორციელებული აქტივობა

შეიძლება სარისკო იყოს. თუ არ ხართ დარწმუნებული ასეთი ქსელების დაცულობაში, ნუ დაკავდებით ისეთი აქტივობებით როგორებიცაა: მნიშვნელოვანი კომუნიკაცია, საბანკო ტრანზაქციების განხორციელება, კონფიდენციალური ფაილების გაზიარება და ა.შ.

### 2.6.10. ფორს-მაჟორულ სიტუაციაში მოქცევის წესი

გახსოვდეთ, რომ თქვენს მობილურ მოწყობილობებს აქვთ უნიკალური იდენტიფიკატორები (მათ შორის: IMEI ნომერი, MAC მისამართი, Serial ნომერი). ჩაინიშნეთ ეს ნომრები და, საჭიროების შემთხვევაში, შესაბამის უწყებებში განაცხადეთ. მათი დახმარებით, შესაძლებელია თქვენი დაკარგული ნივთის პოვნა სამართალდამცავებისა და მობილური/ინტერნეტ პროვაიდერების დახმარებით.

თანამედროვე მობილურ მოწყობილობებს აქვთ კატასტროფულ სიტუაციებში ავტომატური ქმედების განხორციელების საშუალება: კერძოდ, რაიმე წინასწარ შერჩეული კომბინაციის აკრეფვისას:

- ავტომატურად გზავნის თქვენს ლოკაციას სამაშველო სამსახურში;
- წინასწარ მითითებულ ნომერზე გზავნის საჭირო სმს შეტყობინებას;
- იღებს ფოტო-ვიდეო მასალას და გზავნის წინასწარ მითითებულ ადრესატთან,
- ჩაშენებული მოდულის მეშვეობით აფიქსირებს თქვენს ვარდნას ან რაიმე სახის ფიზიკურ ინციდენტს;

გაეცანით ზემოთ მოყვანილ წესებს და გახსოვდეთ, ზოგჯერ მობილური მოწყობილობა მხოლოდ ციფრული კომუნიკაციის საშუალება არ გახლავთ.

საქართველოს სტრატეგიის და განვითარების ცენტრი

www.gcsd.org.ge
gcsd@gcsd.org.ge
032 2 22 26 67
მცხეთის ქუჩა #48/50