რას უნდა მიაქციოთ ყურადღება MFA-ს ჩართვამდე

• **MFA მნიშვნელოვნად ზრდის უსაფრთხოებას** — მის გარეშე თავდამსხმელებს შეუძლიათ გატეხონ პაროლი და მიიღონ წვდომა ანგარიშზე. (CRN)
• არსებობს ორი ძირითადი მიდგომა: **per-user MFA** (მომხმარებლების მიხედვით ჩართვა) და **წვდომის წესების გამოყენება** (მაგალითად, პირობითი წვდომის პოლიტიკები).
• თქვენ უნდა გქონდეთ **ადმინისტრატორის უფლებები** (მაგალითად, გლობალური ადმინისტრატორი ან უსაფრთხოების ადმინისტრატორი).
• მომხმარებლები მზად უნდა იყვნენ დააყენონ **დამატებითი ავთენტიფიკაციის მეთოდი** (ტელეფონი, ავთენტიფიკატორის აპლიკაცია და ა.შ.).

MFA-ს ჩართვის ეტაპები

ქვემოთ მოყვანილია ძირითადი მეთოდები — შეგიძლიათ აირჩიოთ თქვენთვის სასურველი მეთოდი.

მეთოდი 1: MFA-ს ჩართვა ცალკეული მომხმარებლებისთვის (per-user)

1. შედით **Microsoft 365 ადმინისტრატორის პორტალზე:** https://admin.microsoft.com
2. გადადით **მომხმარებლები → აქტიური მომხმარებლები** (Users → Active users). *(NinjaOne)*
3. აირჩიეთ ის მომხმარებელი(ები), ვისთვისაც გსურთ MFA-ს ჩართვა.
4. დააჭირეთ ბმულს ან ღილაკს **მრავალფაქტორიანი ავთენტიფიკაცია (Multi-factor authentication)**. *(ManageEngine)*
5. გახსნილ ფანჯარაში აირჩიეთ მომხმარებლის სტატუსი: **Enabled (ჩართული)** ან **Enforced (სავალდებულო)**. *(NinjaOne)*
6. შემდეგი ავტორიზაციის დროს მომხმარებელი გადამისამართდება MFA-ს დაყენების ეკრანზე, სადაც აირჩევს მეთოდს (აპლიკაცია, SMS, ზარი და ა.შ.) და გააქტიურებს მას.

მეთოდი 2: MFA-ს პარამეტრების გამოყენება Microsoft Entra ID პორტალის მეშვეობით (ადრე Azure AD)

1. შედით **Microsoft Entra Admin Center**-ში.
2. გადადით: **Entra ID → Authentication methods** ან **Entra ID → Multi-factor authentication**. *(Microsoft Learn)*
3. პარამეტრების გვერდზე შეგიძლიათ:
    - დააყენოთ ავთენტიფიკაციის მეთოდები (SMS, ზარი, აპლიკაცია) *(Microsoft Learn)*
    - განსაზღვროთ გამონაკლისები (სანდო IP მისამართები) — მაგალითად, ოფისიდან შესვლისას კონკრეტული IP დიაპაზონიდან. *(Microsoft Learn)*
    - ჩართოთ წესი **„მოწყობილობის/ბრაუზერის დამახსოვრება“**, რათა MFA ხელახლა არ მოითხოვოს გარკვეული დღეების განმავლობაში. *(Microsoft Learn)*

მეთოდი 3: პირობითი წვდომის პოლიტიკის (Conditional Access) გამოყენება

• **Microsoft Entra**-ში შეგიძლიათ შექმნათ პირობითი წვდომის პოლიტიკა, რომელიც მოითხოვს MFA-ს გარკვეულ პირობებში — მაგალითად, როცა შესვლა ხდება უცნობი მოწყობილობიდან ან სხვა გეოლოკაციიდან. *(Microsoft Learn)*
• უსაფრთხოების გასაძლიერების მიზნით რეკომენდებულია ამ მიდგომის კომბინაცია **ძველი ავთენტიფიკაციის (legacy authentication)** დაბლოკვასთან. *(NinjaOne)*

MFA-ს ჩართვის შემდეგ: შემოწმება და მხარდაჭერა

• გადაამოწმეთ MFA-ს სტატუსი ყველა მომხმარებლისთვის — ვის აქვს გააქტიურებული და ვის არა.
• დარწმუნდით, რომ მომხმარებლებმა მიიღეს ინსტრუქციები: როგორ დააყენონ ავთენტიფიკატორის აპლიკაცია და როგორ გამოიყენონ სარეზერვო მეთოდი.
• შექმენით სია იმ მომხმარებლების, ვისაც შეუძლია **MFA-ს გადაყენება ან პრობლემების მოგვარებაში დახმარება**.
• ჩართეთ მონიტორინგი: დააკვირდით შესვლის მცდელობებს, რომლებიც მოითხოვენ MFA-ს, და დააფიქსირეთ გამონაკლისები.
• რეგულარულად გადაამოწმეთ პარამეტრები — შესაძლოა საჭირო გახდეს პოლიტიკების ან მეთოდების განახლება (მაგალითად, SMS კოდის ამოღება, თუ გამოჩნდა უფრო უსაფრთხო ალტერნატივა).