

ეკრანს მიღმა:

**მედუზობა, თვით
და კოლექტიური
ზრუნვა ციფრულ ეკოქაში**

სარჩევი

ეკრანს მიღმა: მედეგობა, თვით და კოლექტიური ზრუნვა ციფრულ ეპოქაში

შესავალი	4
ონლაინ ძალადობა და ციფრული კეთილდღეობა	6
რა არის ტექნოლოგიების გამოყენებით ჩადენილი გენდერული ძალადობა?	6
როგორ დავიცვათ ბალანსი ონლაინ აქტივიზმსა და ციფრულ კეთილდღეობას შორის?	7
ონლაინ სივრცე და ჩვენი იდენტობა	8
რა არის ციფრული თავდასხმა?	9
რა არის ციფრული ჰიგიენა?	10
ონლაინ ინსტრუმენტების უსაფრთხო გამოყენება	12
ტექნოლოგიებით ჩადენილი გენდერული ძალადობის [TFGBV] დოკუმენტირების საუკეთესო პრაქტიკები	14
სათემო ზრუნვა და უსაფრთხო სივრცეების შექმნა	23
როგორ დავნერგოთ თემზე ზრუნვის პრაქტიკა?	26
უსაფრთხო ონლაინ და ფიზიკური სივრცეების შექმნა	28
უსაფრთხო სივრცის პრინციპები	28
უსაფრთხო ონლაინ სივრცეების შექმნა	30
უსაფრთხო პროექტის მართვა:	32
მონაცემთა დაცვა:	32
კოლექტიური ზრუნვის შენარჩუნება	33
არაძალადობრივი კომუნიკაცია	33
არ ავნო პრინციპის დანერგვა	36
თვითზრუნვის პრაქტიკები	37
რა არის მედიტაცია?	40
სტრესი	50
რეკომენდაციები: როგორ დავნერგო მაინდფულნესი ყოველდღიურად:	60
პრაქტიკული მექანიზმები და სამუშაო პროტოკოლები	61

ორგანიზაციის უსაფრთხოების პროტოკოლი	61
ციფრული უსაფრთხოების შიდაგანაწესი	62
ზრუნვაზე დაფუძნებული სამუშაო სივრცე - პროტოკოლი	64
ტექნოლოგიების გამოყენებით ჩადენილი ძალადობის მონიტორინგის პროტოკოლის კითხვარი	68
გაცნობიერებული თვითზრუნვის სკალა	70
წყაროები	78

შესავალი

ციფრული გარემო სწრაფად ვითარდება და მასთან ერთად იზრდება გამოწვევები, რომლებიც ადამიანის კეთილდღეობასა და უსაფრთხოებას ეხება. წიგნი რომელიც თქვენ წინაშეა, წარმოადგენს სახელმძღვანელოს ციფრული ძალადობის, ციფრული ჰიგიენის, თვითზრუნვისა და თემზე ზრუნვის შესახებ. მისი მიზანია, დაეხმაროს აქტივისტებსა და ორგანიზაციებს ონლაინ და ოფლაინ სივრცეებში უსაფრთხო, არაძალადობრივი და მზრუნველობითი გარემოს შექმნაში.

ეს პრაქტიკული სახელმძღვანელო ეფუძნება ადგილობრივ და საერთაშორისო გამოცდილებას და მიზნად ისახავს ცოდნის, ინსტრუმენტებისა და კონკრეტული მექანიზმების გაზიარებას იმ ადამიანებისთვის, ვინც ზრუნავს საკუთარ თავზე, თავიანთ თემზე და უსაფრთხო სამუშაო გარემოს შექმნაზე.

წიგნის მიზანია:

- ცნობიერების ამაღლება ციფრული ძალადობის ფორმებისა და შედეგების შესახებ;
- ციფრული უსაფრთხოების საბაზისო პრინციპების მიწოდება მარტივი და პრაქტიკული ფორმით;
- თვითზრუნვის და თემზე ზრუნვის კულტურის გაძლიერება ორგანიზაციულ და პიროვნულ დონეზე;
- არაძალადობრივი კომუნიკაციის და ურთიერთობის განვითარება;
- ორგანიზაციებისთვის უსაფრთხოების პროტოკოლებისა და ზრუნვაზე დაფუძნებული მიდგომების დანერგვის ხელშეწყობა.

წიგნი განკუთვნილია:

- საზოგადოებრივი და უფლებადამცველი ორგანიზაციებისთვის;
- აქტივისტებისთვის და მოძრაობების წევრებისთვის;
- განათლების სფეროში მოღვაწე პირებისთვის;
- იმ ადამიანებისთვის, ვინც ყოველდღიურად იყენებს ციფრულ სივრცეს და სურს თავი დაცულად იგრძნოს ონლაინ და ოფლაინ.

ეს სახელმძღვანელო განსაკუთრებით გამოსადეგია იმ ჯგუფებისთვის, ვინც მუშაობს სხვადასხვა თემის მხარდაჭერაზე, და სურს შექმნას უსაფრთხო, მზრუნველობითი და არაძალადობრივი სამუშაო გარემო.

როგორ გამოვიყენოთ წიგნი?

წიგნი დაყოფილია თემატურ ნაწილებად, რაც საშუალებას გაძლევთ წაიკითხოთ მასალები საჭიროების მიხედვით – თანმიმდევრობით ან კონკრეტული თავის მიხედვით. მისი გამოყენება შესაძლებელია როგორც ინდივიდუალურ სწავლისთვის, ისე ჯგუფური შეხვედრების, ტრენინგების ან შინაგანაწესების განახლების პროცესში.

მნიშვნელოვანია:

- გადაიაზროთ სახელმძღვანელოს შინაარსი თქვენი ორგანიზაციის სპეციფიკის მიხედვით;
- გამოიყენოთ პრაქტიკული თავები (მაგ. “უსაფრთხო სივრცეების შექმნა”, “თვითზრუნვა”, “ციფრული ჰიგიენა”) შიდა სახელმძღვანელოების შესამუშავებლად;
- ჩართოთ თანამშრომლები წიგნის განხილვაში, რათა გაზარდოთ საერთო ჩართულობა და მზრუნველობითი კულტურა.

როგორ დავნერგოთ ორგანიზაციაში?

- წიგნის წარმატებით დანერგვისთვის ორგანიზაციაში, რეკომენდებულია:
- შიდა ტრენინგების და სამუშაო შეხვედრების ჩატარება წიგნის თემებზე;
- უსაფრთხოების შიდა პროტოკოლების შედგენა და/ან განახლება, გამოყენებით წიგნის შესაბამისი თავებისა (“ციფრული უსაფრთხოების შიდაგანაწესი”, “უსაფრთხო სივრცის პრინციპები”);
- კოლექტიური ზრუნვის პრაქტიკის ჩამოყალიბება, რომელიც მოიცავს რეგულარულ მხარდაჭერის სივრცეებს გუნდისთვის;
- არაძალადობრივი კომუნიკაციის ტრენინგები და რეფლექსიის სესიები;
- ციფრული უსაფრთხოების რეკომენდაციების ინტეგრაცია ყოველდღიურ სამუშაო პროცესში – მაგალითად, პაროლების მართვა, მონაცემთა დაცვა, უსაფრთხო კომუნიკაცია და სხვა.
- თვითზრუნვის ხელშეწყობა როგორც ინდივიდუალური, ისე გუნდური დონეზე.

რატომ ვართ დაუცველები?

- ვიყენებთ მარტივ და განმეორებად პაროლებს
- არ ვაახლებთ პროგრამებს დროულად
- ვაჭერთ უცნობ ბმულებს
- არ ვიყენებთ ორმაგ ავთენტიფიკაციას
- გვჯერა, რომ “ეს მე არ შემეხება”

სინამდვილეში, ნებისმიერი ადამიანი ან ორგანიზაცია შეიძლება გახდეს სამიზნე.

ციფრული თავდასხმებისგან თავის დაცვა იწყება ცოდნით. სანამ რაიმე ზომებს მივმართავთ, პირველ რიგში უნდა გავიგოთ:

- როგორ მუშაობს ციფრული საფრთხე
- როგორ უნდა დავაკვირდეთ საეჭვო ქცევებს
- როგორ დავიცვათ ჩვენი ინფორმაცია ყოველდღიურობაში

რა არის ციფრული ჰიგიენა?

ციფრული ჰიგიენა იგივეა, რაც პირადი ჰიგიენა — მაგრამ ვირტუალურ სივრცეში.

ის მოიცავს ისეთ ქცევებსა და ჩვევებს, რომლებიც გვეხმარება:

- დავიცვათ ჩვენი მონაცემები
- ავიცილოთ ვირუსების მავნე გავლენა და კიბერთავდასხმები
- ვიყოთ უსაფრთხოდ ინტერნეტ სივრცეში

ციფრული ჰიგიენა არის **ციფრულ სამყაროში უსაფრთხოდ ცხოვრების წესის სწავლა.**

ციფრული უსაფრთხოების 10 ძირითადი წესი



გამოიყენე რთული და უნიკალური პაროლები

არ გამოიყენო ერთი და იგივე პაროლი რამდენიმე საიტზე.
- გამოიყენე დიდი ასოები, ციფრები და სიმბოლოებს შორის კომბინაცია.
- გამოიყენე პაროლების მმართველი პროგრამები (მაგ. Bitwarden, 1Password).



ჩართე ორფაქტორიანი ავთენტიფიკაცია (2FA)

გარდა პაროლისა, დამატებითი დაცვაა –
ჩვეულებრივ კოდი, რომელიც მოდის SMS-ით ან აპით.



არ გახსნა საეჭვო ბმულები და ფაილები

ელ.ფოსტით ან მესენჯერში მიღებული უცნობი ბმულები ხშირად ფიშინგია.
თუ რამე საეჭვოა — არ დააჭირო!



არ გაუზიარო შენი პირადი ინფორმაცია ყველას

გადამონებული წყაროს გარდა, არავის გაუმხილო:

- პაროლები
- საბანკო მონაცემები
- პირადი ნომერი



დააყენე პროგრამული განახლებები დროულად

პროგრამები ხშირად შეიცავს ხარვეზებს
— განახლებები ამ ხარვეზებს აღმოფხვრის.
— არასოდეს გამოიყენო “update later”!



დააყენე ანტივირუსი და firewall

ისინი ამოიცნობენ და ბლოკავენ მავნე პროგრამებს.
გამოიყენე სანდო ანტივირუსი და არ გადმოწერო საეჭვო წყაროებიდან.



გამოიყენე უსაფრთხო Wi-Fi კავშირი

არ შეხვიდე პირად ანგარიშებზე საზოგადოებრივი Wi-Fi-ით, თუ არ იყენებ VPN-ს.
შენი მონაცემები შეიძლება მარტივად მოიპარონ დაუცველ ქსელებზე.



რეგულარულად გააკეთე სარეზერვო ასლები

თუ ვირუსი ან შეცდომა ფაილებს გაანადგურებს, ასლი გადაგარჩენს. გამოიყენე დრუბლოვანი ან გარე საცავი.



შეამოწმე შენს ანგარიშებზე აქტივობა

ბანკის, იმეილის ან სოციალური ქსელის ანგარიშებზე რეგულარულად გადახედე:

- ბოლო შესვლებს
- უცნობ მოწყობილობებს
- უცნაურ ქცევებს



გაანათლე საკუთარი თავი და სხვებიც

იცოდე, როგორ მუშაობს ფიშინგი, სპამი, ვირუსი და სხვა საფრთხეები. ცოდნა — შენი ყველაზე ძლიერი იარაღია.

ონლაინ ინსტრუმენტების უსაფრთხო გამოყენება

1. შეამოწმე და შეზღუდე შენი პროფილის ხილვადობა

- დააყენე პროფილი “მხოლოდ მეგობრებისთვის” (private), არა ყველასთვის (public).
- აკონტროლე, ვინ ხედავს:
 - შენს პოსტებს
 - მეგობრების სიას
 - ფოტოს, დაბადების თარიღს და ადგილმდებარეობას
 - რაც ნაკლები ინფორმაციაა საჯაროდ, მით უფრო დაცული ხარ.

2. არ განათავსო მგრძნობიარე ინფორმაცია

ნუ აქვეყნებ:

- პირადობის ნომერს
- საბანკო მონაცემებს
- მისამართს ან ნომერს
- ადგილმდებარეობას რეალურ დროში (“ახლა ხან ჩამოვედი ბათუმში” = მოწვევა ძარცვისთვის)
- გახსოვდეს: რაც ერთხელ “დაგეპოსტა”, სამუდამოდ ინტერნეტში რჩება.

3. გამოიყენე ძლიერი პაროლი და ჩართე ორფაქტორიანი ავთენტიფიკაცია (2FA)

- არასოდეს გამოიყენო პაროლი: 123456, qwerty ან საკუთარი სახელი.
- ჩართე დამატებითი დაცვა — მაგალითად, კოდი, რომელიც SMS-ით ან აპით მოდის შესვლისას.

ეს განსაკუთრებით მნიშვნელოვანია Instagram, Facebook, TikTok და LinkedIn-ისთვის.

4. გაფრთხილდი ფიშინგისგან

- თუ მიიღე უცნაური ბმული მეგობრისგან ან უცნობი პირისგან — არ დააჭირო!
- სოციალურ ქსელშიც არსებობს მავნე ბმულები, რომლებიც პაროლებს იპარავენ.
- ოფიციალური გვერდები არასდროს მოგთხოვენ პაროლს მესენჯერით.

5. დააკვირდი ანგარიშზე უცნაურ აქტივობას

- ახალი ლოკაცია შესვლებში? უცნობი მოწყობილობა? უცნაური კომენტარები შენს სახელით?
- ➔ დაუყოვნებლივ შეცვალე პაროლი და გამოედი ყველა მოწყობილობიდან.

6. არ მიიღო ყველა მომთხოვნი მეგობრობაში

- ბევრი ყალბი ანგარიში შენს პროფილზე ინფორმაციას აგროვებს.
- მეგობრებში მხოლოდ ის ადამიანები დაიმატე, ვინც რეალურად იცნობ ან ენდობი.

თუ დაიცავ ზემოთ ჩამოთვლილ წესებს, იქნები ბევრად დაცული და ნაკლებად მოწყვლადი კიბერ საფრთხეების მიმართ.

ზოგადი (3 კითხვა)

ბოლო შვიდი დღის განმავლობაში,

ჩავერთე თვითზრუნვის სხვადასხვა აქტივობაში.

1	2	3	4	5
---	---	---	---	---

დავგეგმე ჩემი თვითზრუნვა.

1	2	3	4	5
---	---	---	---	---

ჩემს ცხოვრებაში თვითზრუნვის ახალი გზები მოვიძიე.

1	2	3	4	5
---	---	---	---	---

ქულათა საერთო ჯამი

დარწმუნდით, რომ სწორად დააფიქსირეთ თქვენი შებრუნებული ქულა.

საშუალო

ქულა

მაინდფულ რელაქსაცია/დასვენება

ფიზიკური ზრუნვა

თვითთანადგომა და დანიშნულება

მხარდამჭერი ურთიერთობები

მხარდამჭერი სტრუქტურა/რუტინა

გაცნობიერება

ზოგადი– 3 სხვადასხვა ქულა:

მრავალფეროვნება

დაგეგმვა

აღმოჩენა

5						
4						
3						
2						
1						
საპლა	რელაქსაცია	ფიზიკური ზრუნვა	თვითთანადგომა	მხარდამჭერი ურთიერთობები	მხარდამჭერი სტრუქტურა	გაცნობიერება

გრძელი ვერსიისთვის შეგიძლიათ იხილოთ შემდეგი წყარო: Cook-Cottone, C. P. (2015). Mindfulness and yoga for embodied self-regulation: A primer for mental health professionals. New York, NY: Springer Publishing.

