პროგრამა

უსაფრთხო ონლაინი: ქალთა გაძლიერება ციფრულ ეკონომიკაში

ტრენინგი

ელექტრონული კომერციის (E-commerce) უსაფრთხოება და ტექნოლოგიებზე დაფუძნებული გენდერული ნიშნით ძალადობა (TFGBV)

დოქტორი ლელა მირცხულავა
უსაფრთხოების/ტექნოლოგიების სპეციალისტი

14 მაისი 2024

რა არის ელექტრონული კომერციის უსაფრთხოება?

❑ელექტრონული კომერციის უსაფრთხოება არის გზამკვლევი, რომელიც უზრუნველყოფს *უსაფრთხო ტრანზაქციებს ინტერნეტის საშუალებით*. ის შედგება *პროტოკოლებისგან*, რომლებიც იცავს იმ ადამიანებს, რომლებიც *ეწევიან საქონლის ან მომსახურეობის ონლაინ გაყიდვასა და ყიდვას.*

❑თქვენ უნდა მოიპოვოთ თქვენი მომხმარებლების ნდობა ელექტრონული კომერციის უსაფრთხოების მექანიზმების დანერგვით, რაც უზრუნველყოფს შემდეგ პროცესებს, როგორიცაა:

- კონფიდენციალურობა
- მთლიანობა
- ავთენტიფიკაცია
- არაუარყოფა

MERCY CORPS

სტატისტიკის მიხედვით

ელექტრონულ კომერციის შემთხვევაში, მთავარი აქცენტი კეთდება მონაცემთა გაცვლაზე ორ მხარეს შორის ინტერნეტის საშუალებით.

ინტერნეტი არ არის იმუნური ყველა სახის კიბერუსაფრთხოების საფრთხეებისა და კიბერშეტევების მიმართ.

სტატისტიკის მიხედვით, 2022 წელს ელექტრონული კომერციის ***ზარალმა 41 მილიარდი აშშ დოლარი შეადგინა***, ხოლო 2023 წელს კი ***48 მილიარდ აშშ დოლარს*** მიაღწია.

ბოლო კვლევები მიუთითებს იმაზე, რომ კიბერდანაშაული იზრდება ზოგიერთი მსხვილი კომპანიებისთვისაც, როგორიცაა Yahoo, Facebook და ა.შ., რომლებიც თვითონ გვევლინებიან კიბერშეტევების მსხვერპლი.

MERCY CORPS

ელ. კომერციის უსაფრთხოების საფრთხეები

აქ მოცემულია უსაფრთხოების რამდენიმე საერთო პრობლემა, რომელიც შეიძლება წარმოიშვას ელექტრონული კომერციის ბიზნესის ფარგლებში:

(1) ფიშინგი:

ფიშინგი არის კიბერშეტევის მეთოდი, რომელიც გულისხმობს ***მომხმარებლის სენსიტიური ინფორმაციის შეგროვებას***, როგორიცაა ***login და საკრედიტო ბარათის დეტალები*** თაღლითური ელფოსტის ან შეტყობინებების გაგზავნის გზით.

(2) ფარმინგი:

ეს შემთხვევა ხშირია . ეს არის კიბერშეტევის ტიპი, სადაც კიბერკრიმინალები ***მომხმარებლებს*** გადაამისამართებენ ორიგინალური ვებსაიტების ნაცვლად ***იდენტურ ყალბ ვებსაიტებზე***, მომხმარებლის ინფორმაციის მოსაპოვებლად.

(3) ვეილინგი

ვეილინგი, იგივე აღმასრულებელი დირექტორთან თაღლითობა, არის ფიშინგის შეტევის ტიპი, სადაც სამიზნე არიან მაღალი დონის ბიზნესის აღმასრულებლები როგორიცაა ***აღმასრულებელი დირექტორი,*** რათა მიიღონ სენსიტიური ინფორმაცია, როგორიცაა ***ფინანსური მონაცემები***.

(4) მავნე პროგრამა:

სენსიტიური ინფორმაციის მოსაპარად ჰაკერებმა შეიძლება გამოიყენონ ***მავნე პროგრამა,*** კომპიუტერული სისტემების გამოსაყენებლად შექმნილი პროგრამული უზრუნველყოფა.

(5) SQL ინექცია:

SQL ინექცია არის *ტექნიკური თავდასხმა,* სადაც კიბერ კრიმინალებს შეაქვთ მავნე კოდი ელექტრონული კომერციის ვებსაიტის მონაცემთა ბაზაში, რათა ***მიიღონ წვდომა მომხმარებელთა ინფორმაციაზე***.

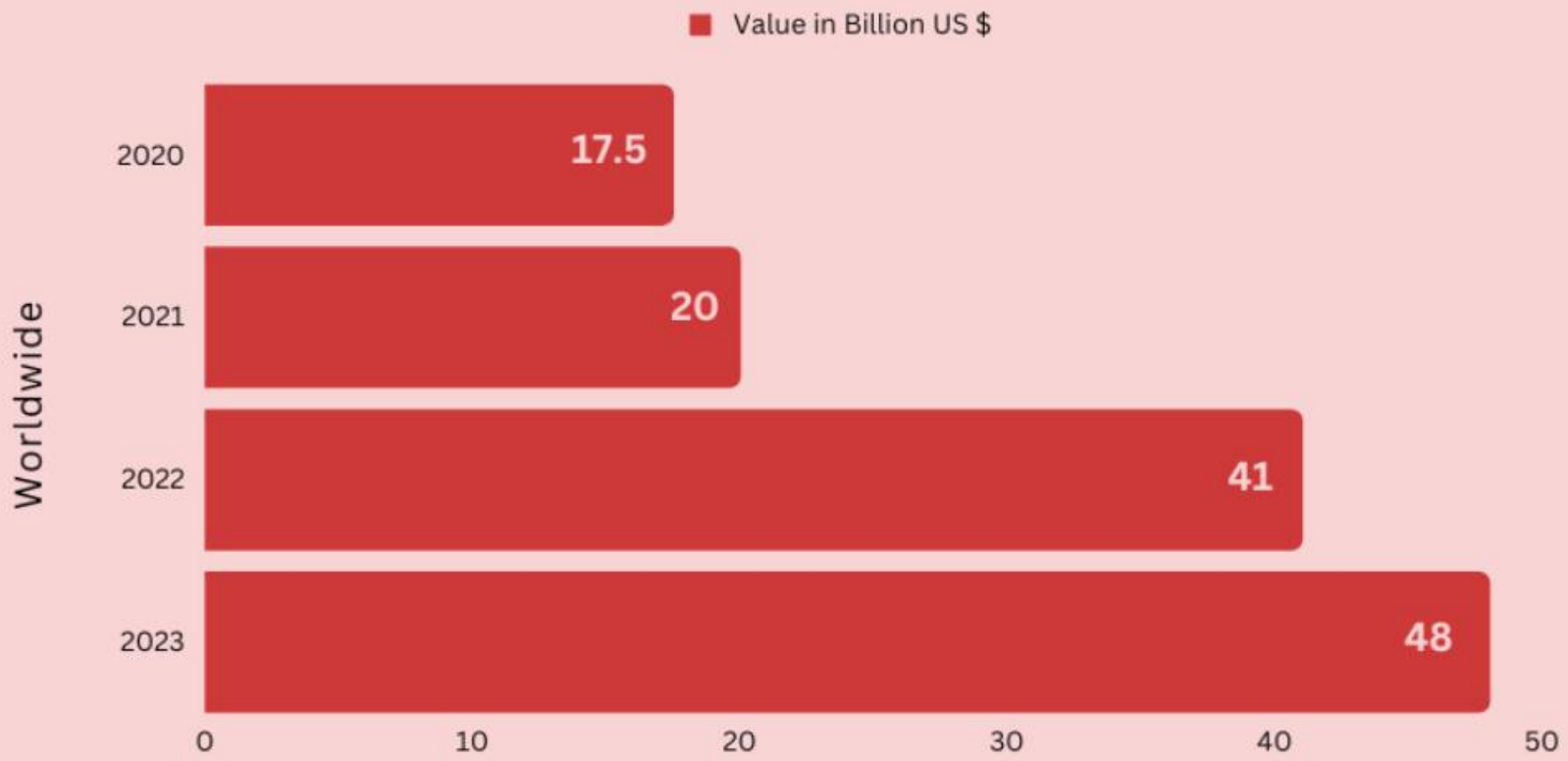
(6) სერვისების უარყოფის განაწილებული (DDoS) შეტევები:

DDoS შეტევები ***გადატვირთავს ვებსაიტების სერვერებს და იწვევს კრახს.*** ამან შეიძლება გამოიწვიოს *გაყიდვების დაკარგვა* და ***ზიანი მიაყენოს ბიზნეს რეპუტაციას.***

MERCY CORPS

Billion US $ Losses Due to Ecommerce Payment Fraud

Source: Statista
Created By: Purchase Commerce



MERCY CORPS

გზა მომავლისკენ

- ***გაერომ*** განაცხადა, რომ *ინტერნეტი უკვე ადამიანთა უფლებების ჩამონათვალშია.* კონკრეტულად, *ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-19 მუხლს* დაემატა შემდეგი ჩანაწერი: *„ყველას აქვს უფლება ჰქონდეს აზრისა და გამოხატვის თავისუფლება; ეს უფლება მოიცავს საკუთარი აზრის გამოხატვის თავისუფლებას ყოველგვარი ჩარევის გარეშე და ასევე მოიძიოს, მიიღოს და გაავრცელოს ინფორმაცია და იდეები ნებისმიერი საშუალებით შეზღუდვების მიუხედავად“.*

- ***გლობალური*** და ***ღია ინტერნეტი*** *არსებითად მნიშვნელოვანია* ***მდგრადი განვითარების მიზნების 2030 (Sustainable Development Goals)*** *მისაღწევად, რაც აღიარებულია ადამიანის უფლებათა საყოველთაო დეკლარაციის მე-19 მუხლით და დემონსტრირებულია როგორც ქვეყნების, ასევე ორგანიზაციების მიერ.*

ადამიანის უფლებათა ევროპული კონვენცია

მუხლი 9

აზრის, სინდისისა და რელიგიის თავისუფლება

1. ყველას აქვს აზრის, სიწდისისა და ◆რელიგიის თავისუფლება. ეს უფლება მოიცავს რელიგიის ან რწმენის შეცვლის თავისუფლებას, აგრეთვე, თავისუფლებას იმისა, რომ ცალკე ან სხვებთან ერთად, საქვეყნოდ ან გაწკერძოებით, გაამჟღავნოს თავისი რელიგია თუ რწმენა აღმსარებლობით, ქადაგებით, წესებისა და რიტუალების აღსრულებით.

2. რელიგიის ან რწმენის გამჟღავნების თავისუფლება მხო ლოდ იმ პირობით შეიზღუდება, თუ ასეთი შეზღუდვა გათვალისწიწებულია კანონით და აუცილებელია დემოკრატიულ საზოგადოებაში საზოგადოებრივი უსაფრთხოების ინტერესებისათვის, საზოგადოებრივი წესრიგის, ჯანმრთელობისა ან მორალის, ანდა სხვათა უფლებებისა და თავისუფლებების დასაცავად.

მუხლი 10

გამოხატვის თავისუფლება

1. ყველას აქვს აზრის გამოხატვის თავისუფლება. ეს უფლება მოიცავს ადამიანის თავისუფლებას, გააჩნდეს საკუთარი შეხედულება, მიიღოს ან გაავრცელოს ინფორმაცია ან იდეები საჯარო ხელისუფლების ჩაურევლად და სახელმწიფო საზღვრების მიუხედავად. ეს მუხლი ვერ დააბრკოლებს სახელმწიფოს, მოახდინოს რადიომაუწყებლობის, ტელევიზიისა და კინემატოგრაფიულ საწარმოთა ლიცენზირება.

2. ამ თავისუფლებათა განხორციელება, რამდენადაც ისინი გაწუყოფელია შესაბამისი ვალდებულებისა და პასუხისმგებლობისაგან, შეიძლება დაექვემდებაროს კანონით დადგენილ ისეთ წესებს, პირობებს, შეზღუდვებს ან სანქციებს, რომლებიც აუცილებელია დემოკრატიულ საზოგადოებაში ეროვნული უშიშროების, ტერიტორიული მთლიანობის ან საზოგადოებრივი უსაფრთხოების ინტერესებისათვის, საზოგადოებრივი უწესრიგობის თუ დანაშაულის აღსაკვეთად, ჯანმრთელობის ან მორალის დაცვის მიზნით, სხვათა უფლებების ან ღირსების დასაცავად, საიდუმლოდ მიღებული ინფორმაციის გამჟღავნების თავიდან ასაცილებლად, ანდა სასამართლოს ავტორიტეტისა და მიუკერძოებლობის უზრუნველსაყოფად.

MERCY CORPS

ელექტრონული კომერციის უსაფრთხოების ზომები

(1) SSL სერთიფიკატების ინსტალაცია

- **SSL (Secure Sockets Layer)** არის პროტოკოლი, რომელიც უზრუნველყოფს უსაფრთხო და დაშიფრულ კომუნიკაციას თქვენი ელექტრონული კომერციის ბიზნეს ვებსაიტსა და მომხმარებლის ვებ ბრაუზერს შორის.

- თქვენს ვებსაიტზე SSL სერთიფიკატის დაყენებით, მომხმარებლების ყველა ***სენსიტიური ინფორმაცია დაშიფრულია და დაცულია კიბერშეტევებისგან***.

- URL-ში ***ბოქლომის ნიშანი*** ადასტურებს SSL ინსტალაციას თქვენს ვებსაიტზე.

MERCY CORPS

2) ორფაქტორიანი ავთენტიფიკაცია

- ამ შემთხვევაში გამოიყენება ორფაქტორიანი ავთენტიფიკაციას ჩვენს Facebook, Instagram, Gmail და სხვა ანგარიშებში.

- გააქტიურეთ ეს ორფაქტორიანი ავთენტიფიკაცია თქვენი ელექტრონული კომერციის ვებსაიტისთვის, პაროლის გარდა. ეს შეიძლება იყოს დამატებითი უსაფრთხოების დონე თქვენი ბიზნეს ანგარიშის დასაცავად.

MERCY CORPS

3) PCI შესაბამისობა

- გადახდის ბარათების ინდუსტრიის მონაცემთა უსაფრთხოების სტანდარტი (PCI DSS) ასახავს უსაფრთხოების სტანდარტებს საკრედიტო ბარათის ინფორმაციის დასამუსავებლად.

- ელექტრონული კომერციის პლატფორმა უნდა შეესაბამებოდეს PCI-ს, რათა უზრუნველყოს თქვენი საკრედიტო ბარათის დეტალების უსაფრთხოდ დამუშავება.

PCI DSS - The Payment Card Industry Data Security Standard

MERCY CORPS

(4) თაღლითობის გამოვლენა

- თქვენი ელექტრონული კომერციის პლატფორმაში აუცილებელია თაღლითობის გამოვლენის ფუნქციის იმპლემენტაცია, რაც მოახდენს საეჭვო ტრანზაქციების იდენტიფიცირებას.

- უჩვეულო ტრანზაქციების ან IP მისამართების დაბლოკვით, შეგიძლიათ დაიცვათ თქვენი ვებ – გვერდი.

(5) უსაფრთხოების განახლებები

- დარწმუნდით, რომ თქვენი ელექტრონული კომერციის პლატფორმა უზრუნველყოფს უსაფრთხოების განახლებებს, რათა თავიდან აიცილოთ საერთო საფრთხეები.

- ამ ზომების განხორციელებით, თქვენ შეგიძლიათ უზრუნველყოთ თქვენი ელექტრონული კომერციის ვებსაიტის უსაფრთხოება.

რა არის ტექნოლოგიებზე დაფუძნებული გენდერული ნიშნით ძალადობა ანუ TFGBV ?

TFGBV-ის განმარტება UNFPA-ის მიერ!

TFGBV არის ძალადობრივი აქტი კონკრეტული პირის თუ პირების მიმართ, ჩადენილი ან განხორციელებული ერთი ან მეტი პირის მიერ ICT (საინფორმაციო და საკომუნიკაციო ტექნოლოგიების) ასევე ციფრული მედიის სრული თუ ნაწილობრივი გამოყენებით.

Are you experiencing technology-facilitated gender-based violence? (youtube.com)

UNFPA - გაეროს მოსახლეობის ფონდი

MERCY CORPS

ტექნოლოგიებით ხელშეწყობილი გენდერული ძალადობის „გაეროს ქალები“-ს და მსოფლიო ჯანდაცვის ორგანიზაციის ექსპერტთა ჯგუფის მიერ შემოთავაზებული განმარტება

“ძალადობის აქტი, ჩადენილი

ერთი ან მეტი პირის მიერ, რაც

დამძიმებულ იქნა საინფორმაციო საკომუნიკაციო

ტექნოლოგიების ან სხვა ციფრული საშუალებების გამოყენებით

რასაც შედეგად მოყვება ან სავარუდოდ მოყვება

ფიზიკური, სექსუალური, ფსიქოლოგიური

სოციალური, პოლიტიკური ან ეკონომიკური ზიანი ან

უფლებათა და თავისუფლებათა დარღვევა“.

ონლაინ გენდერული ნიშნით ძალადობა vs ონლაინ ძალადობა

ონლაინ გენდერული ნიშნით ძალადობა

TFGBV არის ძალადობის ნებისმიერი ფორმა, რომელიც განხორციელებულია ან ჩადენილი ტექნოლოგიის ან ციფრული ინტერფეისის გამოყენებით - კონკრეტულად ინტერნეტის ან ჭკვიანი მოწყობილობების მეშვეობით, რომლებიც *სამიზნეს ირჩევენ გენდერული ნიშნის, სქესის და სექსუალური ორიენტაციის მიხედ*ვით.

vs

ონლაინ ძალადობა

საყოველთაოდ ცნობილი, როგორც კიბერძალადობა ანუ ძალადობა ტექნოლოგიების გამოყენებით არის ძალადობის ფორმა, რომელიც ხორციელდება კომპიუტერული სისტემების გამოყენებით ცალკეულ ინდივიდებზე ძალადობის, შევიწროების ან დაშინების მიზნით, რაც იწვევს (ან შესაძლოა გამოიწვიოს) ფიზიკურ, სექსუალურ, ფსიქოლოგიურ ან ეკონომიკურ ზიანს ან ტანჯვას, დაფუძნებულს მსხვერპლის გარემოებებიდან თუ დაუცველობიდან გამომდინარე.

MERCY CORPS

გენდერული ძალადობა vs ტექნოლოგიებით განხორციელებული გენდერული ძალადობა

❑ **დიდი ხანია აღიარებულია, რომ გენდერული ძალადობა შესაძლოა მოიცავდეს შემდეგი სახის ძალადობებს:**

- ფიზიკური
- სექსუალური
- ფსიქოლოგიური
- ეკონომიკური

❑ **სულ უფრო და უფრო აღიარებენ, რომ ძალადობის ეს ფორმები შესაძლოა ხელშეწყობილ იქნას ტექნოლოგიების გამოყენებით და მას შეუძლია მოახდინოს ძალადობის მზარდი ფორმების ფასილიტირება, რაც მოიცავს, მაგრამ არ შემოიფარგლება შემდეგით:**

- პირადი/ინტიმური სურათების უნებადრთვო გაზიარება
- პირადი კომუნიკაცია ან პერსონალური მონაცემები
- სექსუალური ძალადობა სურათების მეშვეობით
- ონლაინ ძალადობა
- ტექნოლოგიებით ხელშეწყობილი ძალადობა
- ტექნოლოგიის სხვადასხვა ფორმების გამოყენება თვალთვალისა და დევნისათვის
- მიზანმიმართული ჰაკერობა

MERCY CORPS

რა არის TFGBV-ის ძირითადი ფაქტორები?

TFGBV-ისთვის დამახასიათებელია ორი ძირითადი ფაქტი:

- გენდერულობა - ქალები და გოგონები ხდებიან თავდასხმის ობიექტები მხოლოდ იმიტომ, რომ ისინი ქალები და გოგონები არიან.

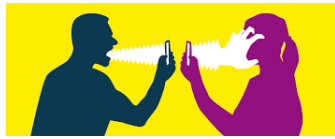
- TFGBV უფრო ფართო მცნებაა, ვიდრე ონლაინ ძალადობა და მიუხედავად იმისა, რომ მოქმედების არეალი ონლაინ სივრცეა, ის ასევე შეიძლება განხორციელდეს:

  - ახალი და ასევე ძველი ტექნოლოგიის გამოყენებით, როგორიცაა ტელეფონები
  - GPS თვალთვალის მოწყობილობები
  - დრონები
  - ჩამწერი მოწყობილობები, რომლებიც ჩართული არ არიან ინტერნეტში.

ვირტუალური სამყარო რეალურია!!!

MERCY CORPS

როგორ გამოიყურება TFGBV რეალურ ცხოვრებაში?



TFGBV შეიძლება განხორციელდეს ახალი ან ძველი ტექნოლოგიების გამოყენებით, მაგრამ ახალი მეთოდებით. ქალთა მიმართ ძალადობა მუდმივად ვითარდება და გვმართებს ვიყოთ ფხიზლად.

TFGBV-ის მრავალი ფორმა არსებობს, მათ შორის აღსანიშნავია:

- ✓ **ონლაინ გენდერული და სექსუალური შევიწროება;**
- ✓ **კიბერსტალკინგი ანუ კიბერადევნება;**
- ✓ **გამოსახულებების ბოროტად გამოყენება, ღრმა ფეიკები ან გენიტალიების არასასურველი გამოსახულებების სხვა პირისთვის გაგზავნა;**
- ✓ **სექსუალური ძალადობა ტექნოლოგიების გამოყენებით ანუ სექსტორაცია (შანტაჟი სექსუალური ინფორმაციის, ფოტოების ან ვიდეოების გამოქვეყნების მუქარით), ონლაინ გრუმინგი სექსუალური ძალადობის მიზნით;**
- ✓ **დოქსინგი (პირადი ინფორმაციის გამოქვეყნება);**
- ✓ **დაჰაკვა - ადამიანების მანიპულირება;**
- ✓ **სექსუალური იმიტაცია;**
- ✓ **სამიზნეების ძიება და ტექნოლოგიის გამოყენება გადარჩენილების მოსაძებნად ძალადობის განსახორციელებლად;**
- ✓ **სიძულვილის ენა - მოიაზრებს გამოხატვის ყველა ფორმას, რომელიც ხელს უწყობს, პროვოცირებას უწევს, ან ამართლებს ქსენოფობიას, რასობრივ შუღლს, ანტისემიტიზმს, შეუწყნარებლობას.**
- ✓ **ცილისწამება;**
- ✓ **გადარჩენილების ტექნოლოგიებთან წვდომის შეზღუდვა ან კონტროლი.**

MERCY CORPS

ძირითადი სტატისტიკა: პოპულარული ციფრულ პლატფორმები

TFGBV-ის მიერ გამოყენებული ციფრული პლატფორმებია:

- ტიკტოკი – 40%
- ინსტაგრამი - 20%
- YouTube, Reddit, and Social gaming platforms - 10%

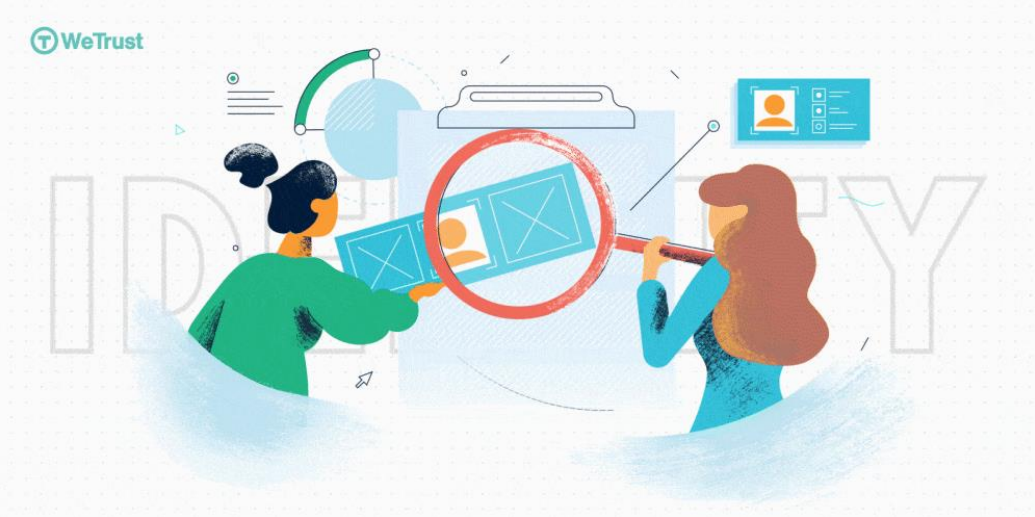
ციფრული ინკლუზია & უსაფრთხოება

ციფრული ინკლუზია შეუძლებელია ციფრული უსაფრთხოების გარეშე![1]

ანუ

- ციფრული პროდუქტებით სარგებლობა შეუძლებელია მომხმარებლების უსაფრთხოებისა და დაცვის უზრუნველყოფის გარეშე.

- ინტერნეტისა და ციფრული პროდუქტების გავრცელებამ გამოავლინა უზარმაზარი შესაძლებლობა ქალებისა და გოგონებისათვის თანაბარი მომავლის შესაქმნელად.



https://blog.wetrust.io/how-digital-identity-will-power-financial-inclusion-69be0d0a0cb0

MERCY CORPS

ციფრული ინკლუზია & TFGBV

- **ციფრული სამყარო** -

  - ერთის მხრივ, *სასიცოცხლოდ მნიშვნელოვან სივრცეს სთავაზობს ქალებს*, რომლებსაც აქვთ თვითგამოხატვის სურვილი და ეძებენ შესაძლებლობებს მიიღონ საბაზისო განათლება და გარკვეულ სერვისებზე წვდომა,

  - მეორეს მხრივ, *არის ვექტორი დამნაშავეებისა და მოძალადეებისთვის* (იგულისხმება ცალკეული პირები, ჯგუფები და კოლექტივები), მიზანმიმართული ქალებისა და მოზარდი გოგონების მიმართ გენდერული ნიშნით ძალადობის (TFGBV) განსახორციელებლად.

რა გავლენას ახდენს TFGBV ?

1

ციფრული სამყარო არის რეალური სამყარო!

- TFGBV ხშირად აღიქმება, როგორც ნაკლებად მძიმე ან ნაკლებად საზიანო ფენომენი, ვიდრე ოფლაინ ძალადობის ფორმები, მაგრამ კვლევა აჩვენებს, რომ მას მოყვება მძიმე შედეგები, *რაც ცუდად აისახება ქალებისა და გოგონების ჯანმრთელობაზე, სიცოცხლეზე და ასევე მათ მომავალზე.*

- TFGBV ასევე ხშირად იწვევს ოფლაინ ძალადობას, რაც ძალზე *საშიშ საფრთხეს უქმნის ქალთა და გოგონების უსაფრთხოებასა და ფიზიკურ შეუხებლობას.*

2

- ***TFGBV-ის გავლენა ფსიქიკურ ჯანმრთელობაზე მძიმეა:***

  - სტრესი;
  - შფოთვა;
  - დეპრესია;
  - პოსტტრავმატული სტრესული აშლილობა;;
  - სუიციდური აზრები;

როგორც წესი, სუიციდზე ინფორმაციას ავრცელებენ თვით გადარჩენილები !!!

3

- ***TFGBV აიძულებს ქალებს იყვნენ ჩუმად ონლაინ სივრცეში***, რაც ამცირებს მათ მონაწილეობას საზოგადოებრივ და პოლიტიკურ ცხოვრებაში, დემოკრატიულ პროცესებში და განსაკუთრებით, ლიდერის როლში.

- *TFGBV აძლიერებს პატრიარქალურ როლებს, ნორმებსა და სტრუქტურებს და ქმნის მთავარ ბარიერს გენდერული თანასწორობისა და მდგრადი განვითარების მიზნების მისაღწევად.*

MERCY CORPS

TFGBV, როგორც კიბერძალადობა

- **TFGBV**, რომელიც ხშირად მოიხსენიება, როგორც ***კიბერძალადობა*** ან ***ონლაინ ძალადობა***, არის *საზოგადოებრივი ჯანდაცვისა და ადამიანთა უფლებების გლობალური პრობლემა*, რომელიც გავლენას ახდენს:

  - ცალკეული პირების უსაფრთხოებაზე
  - მათ კეთილდღეობაზე
  - უარყოფითად მოქმედებს მთლიან საზოგადოებაზე.

MERCY CORPS

რატომ არის კიბერძალადობა გენდერული?

- **კიბერძალადობა** არის ქალებისა და გოგონების მიმართ ძალადობის უწყვეტი ნაწილი და წარმოადგენს ძალადობის და გაჩუმების კიდევ ერთ ფორმას, რომელიც ჩაშენებულია არსებული გენდერული ძალაუფლების სტრუქტურებში.

- ასევე, არსებობს კიბერძალადობის მრავალი ფორმა, რომელიც *ექსკლუზიურად მხოლოდ ქალებისა და გოგოებისკენ არის მიმართული.*

- EIGE-ს კვლევამ გენდერული თანასწორობისა და დიგიტალიზაციის შესახებ ევროკავშირში ხაზგასმით გამოავლინა დიგიტალიზაციის ახალი გენდერული გამოწვევები, მათ შორის ადრეული ასაკის ქალები იყვნენ კიბერძალადობის პოტენციური სამიზნეები.

- ხშირად ციფრული სივრცის მიტოვების შედეგად, კიბერძალადობა დამანგრეველ გავლენას ახდენს ქალთა თავდაჯერებულობაზე, როდესაც საქმე ტექნოლოგიას ეხება, უფრო მეტად რთულდება გენდერული თანასწორობის საკითხების გადაჭრა, როგორიცაა STEM/ICT გენდერული სეგრეგაცია და გენდერული სხვაობა ანაზღაურებაში.

MERCY CORPS

კიბერძალადობის (CVAWG) ფორმები

კიბერ ძალადობა ქალებისა და გოგონების მიმართ (CVAWG) მოიცავს ძალადობის სხვადასხვა ფორმებს, რომლებიც ჩადენილია ICT-ის (ინფორმაციული საკომუნიკაციო ტექნოლოგიების) საშუალებით გენდერული ნიშნის ან სხვა ფაქტორების კომბინაციით (რასა, ასაკი, შეზღუდული პასუხისმგებლობა, სექსუალობა, პროფესია ან პიროვნული რწმენა).

CVAWG-ის ყველა აქტი:

- იწყება ონლაინ და გრძელდება ოფლაინ, მაგალითად, სამუშაო ადგილზე, სკოლაში ან სახლში;
- იწყება ოფლაინ და გრძელდება სხვადასხვა ონლაინ პლატფორმებზე, როგორიცაა სოციალური მედია, ელფოსტა ან მესინჯერები და ე.წ. ჩათები
- ჩადენილია უცნობ პირთა და/ან ანონიმურ ადამიანთა ჯგუფის მიერ;
- ჩადენილია პირის ან ადამიანთა ჯგუფის მიერ, რომლებიც ცნობილია მსხვერპლისთვის, ისინი შეიძლება იყვნენ (ყოფილი) ინტიმური პარტნიორები, სკოლელები ან თანამშრომლები.

MERCY CORPS

ქალებისა და გოგონების კიბერშევიწროება (Cyber harassment)

- ქალებისა და გოგონების კიბერშევიწროება მოიცავს ერთ ან მეტ ქმედებას, ჩადენილს მსხვერპლის მიმართ *მათი გენდერის, ან სქესის და სხვა რიგი ფაქტორების* (მაგ. რასა, ასაკი, ინვალიდობა, პროფესია, პირადი შეხედულებები ან სექსუალური ორიენტაცია) გამო.

- კიბერ-შევიწროება, რომელიც შეიძლება მოიცავდეს *სოციალური მედიაპლატფორმების, ელ-ფოსტის ან მოკლე ტექსტური შეტყობინებების გამოყენებას* მსხვერპლისთვის მუქარის შემცველი, სექსუალური ხასიათის ან შეურაცხმყოფელი შეტყობინებების გაგზავნის მიზნით.

2019 FRA (ევროკავშირის ფუნდამენტური უფლებების სააგენტო)-ს გამოკითხვის თანახმად, ქალების 13%-მა ევროკავშირში, დიდ ბრიტანეთში და ჩრდილოეთ მაკედონიაში განიცადა კიბერშევიწროება წინა 5 წლის განმავლობაში. მსხვერპლნი უფრო ხშირად არიან ახალგაზრდა რესპონდენტები (18-დან 29 წლამდე, ახალგაზრდა ქალების 20%) და შეზღუდული შესაძლებლობის მქონე პირები

MERCY CORPS

კიბერბულინგი გოგონების წინააღმდეგ

კიბერბულინგი (Cyber Bullying) არის ერთი ადამიანის ან ადამიანთა ჯგუფის მიერ, ციფრული კომუნიკაციის საშუალებით (მობილური ტელეფონი, პლანშეტი, კომპიუტერი, ინტერნეტი და ა.შ.), *სხვა ადამიანის ან ადამიანთა ჯგუფის დამცირება*, მათ შესახებ *ცრუ ინფორმაციის გავრცელება*, *პერსონალური მონაცემების არანებაყოფლობითი გამჟღავნება*, *დაცინვა*, *ადევნება*, *შეურაცხყოფა*, *შევიწროება*, *ემოციური* და *ფსიქოლოგიური ზეწოლა*, *მუქარა*, *დაშინება*, რაც მის/მათ გულისტკენას, გაბრაზებას, შეშინებას და/ან წყენას იწვევს.

კიბერბულინგის ძირითადი პლატფორმებია:

- ✓ სმს/ მოკლე ტექსტური შეტყობინება;
- ✓ ონლაინ მესენჯერი/ჩათი;
- ✓ ელექტრონული ფოსტა;
- ✓ სოციალური მედია;
- ✓ ონლაინ ფორუმი;
- ✓ ონლაინ თამაში.

MERCY CORPS

ონლაინ სიძულვის ენა გენდერული ნიშნით

- ***ევროპის საბჭოს მინისტრთა კომიტეტის*** 1997 წ
  მიღებული რეკომენდაციის თანახმად, ***სიძულვილის მოიაზრებს*** გამოხატვის ყველა ფორმას, რომელ
  ავრცელებს, აქეზებს, ხელს უწყობს ან ამართლებს *რასობ
  შუღლს, ქსენოფობიას, ანტისემიტიზმს
  შეუწყნარებლობაზე დაფუძნებული შუღლის სხვა ფორმ
  ნაციონალიზმის, ეთნოცენტრიზმის, დისკრიმინაციისა
  უმცირესობათა ან მიგრანტთა მიმართ გამოხატუ
  მტრობის ჩათვლით.*

!!! მნიშვნელოვანია იმ მეთოდების ცოდნა, რომლებსაც რადიკალური ჯგუფები საზოგადოებაში შეუწყნარებლობის ატმოსფეროს შექმნისა და სხვადასხვა ჯგუფების მიმართ სიძულვილის გაღვივების მიზნით იყენებენ.

MERCY CORPS

არაკონსენსუალური ინტიმური გამოსახულებების ბოროტად გამოყენება (Non-consensual intimate image abuse)

- არაკონსენსუალური ინტიმური გამოსახულების (NCII) ბოროტად გამოყენება იგგვე ძალადობაა ქალებისა და გოგოების მიმართ, რაც გულისხმობს ქალის ან გოგოს ინტიმური, პირადი და/ან მანიპულირებული სურათების/ვიდეოების გავრცელებას ინფორმაციულ კომუნიკაციური ტექნოლოგიების (ICT) საშუალებებით ან ICT საშუალებებით გავრცელების საფრთხეს სუბიექტის თანხმობის გარეშე.

- ტექნოლოგიური მიღწევები სურათების უფრო და უფრო რეალისტურ მანიპულირების საშუალებას იძლევა. ეს შეიძლება განხორციელდეს პროგრამული უზრუნველყოფის გამოყენებით, როგორიცაა Photoshop ან ***AI ინსტრუმენტები***, რათა შეიქმნას სინთეტიკური მედია, როგორიცაა ***deepfakes.***

ონლაინ ძალადობა მიღწევადია!

TFGBV ან OGBV პრევენცია ისევე შესაძლებელია, როგორც GBV-ის ნებისმიერი სხვა ფორმა!

- კვლევებმა აჩვენა, რომ ***პრევენციული ძალისხმევა*** მიმართულია ყველა დონეზე, მათ შორის მთავრობებზე, კერძო სექტორზე, ტექნიკურ კომპანიებზე, თემებზე და ინდივიდებზე.

- გადარჩენილთათვის ადეკვატური რეაგირების სერვისებმა შეიძლება აღმოფხვრას OGBV.

!!! მეტი ქალის და გოგონას ჩართვა STEM (მეცნიერება, ტექნოლოგია, მათემატიკა, ინჟინერია) სფეროებში; ***ქალების ხელმძღვანელობით*** მოქმედი ***ტექნიკური კომპანიების მხარდაჭერა*** და გენდერის ინტეგრირება ჩვენს ამჟამინდელ ტექნოლოგიურ ეკოსისტემაში, მათ შორის AI (ხელოვნური ინტელექტი), კიდევ უფრო შეუწყობს ხელს გენდერულად ბრმა და გენდერულად მიკერძოებული ტექნიკური ეკოსისტემების დეკონსტრუქციას და საბოლოოდ დაეხმარება ***გენდერული ტრანსფორმაციული ეკოსისტემის შექმნას.***

MERCY CORPS

როგორ შევამციროთ TFGBV

- TFGBV არ არის მხოლოდ ონლაინ, არამედ გულისხმობს ციფრული პროდუქტებისა და მოწყობილობების გამოყენებას.

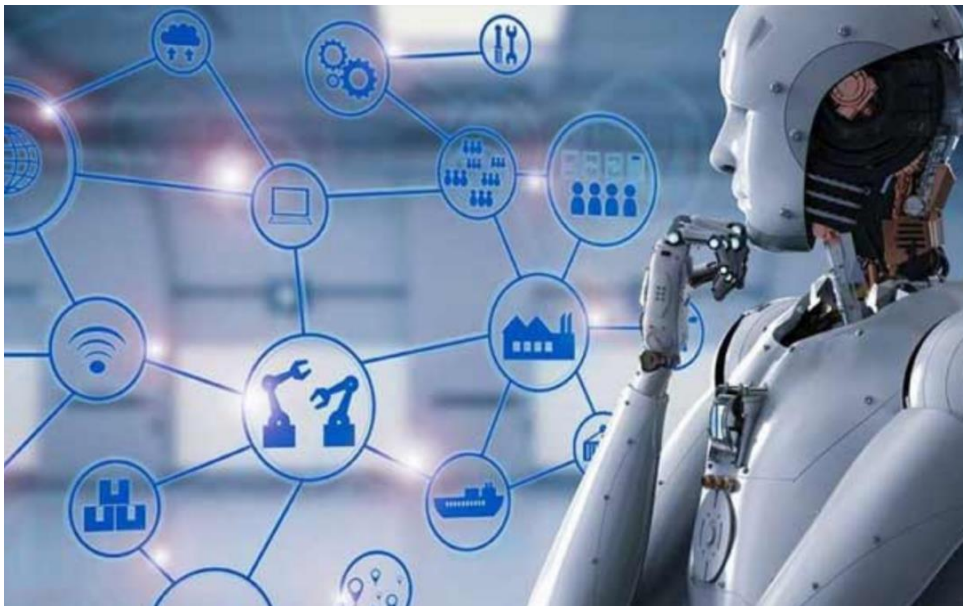
- ურთიერთდაკავშირებული მოწყობილობების ან ნივთების ინტერნეტის (IOT) მოწყობილობების მზარდი გამოყენება და მოთხოვნა გვთავაზობს მეტ სარგებელს, რაც მნიშვნელოვნად აუმჯობესებს ცხოვრების ხარისხს და ზრდის გარკვეული ამოცანების ეფექტურობას.

!!! IOT მოწყობილობებმა *შეიძლება შეაგროვონ და შეინახონ დიდი რაოდენობით მონაცემები და მეტამონაცემები ქალებისა და გოგონების შესახებ* და გაუზიარონ სხვა პირებს, რომლებსაც შეუძლიათ მიიღონ *მონაცემები ქალებისა და გოგონების ადგილსამყოფელის შესახებ, ასევე მოიპოვონ მათი სურათები თუ ვიდეო გამოსახულებები!*

MERCY CORPS

როგორ შევაჩეროთ კიბერბულინგი ხელოვნური ინტელექტის (AI) გამოყენებით

- AI გვაძლევს უამრავ შესაძლებლობას კიბერბულინგის გამოსავლენად:
  - მანქანური სწავლების (ML) და ღრმა სწავლების (DL) ალგორითმებს შეუძლიათ კიბერბულინგის ***ადრეული ნიშნების ამოცნობა***.
  - ***AI ხელს უშლის კიბერბულინგის შემდგომ გავრცელებას***.
  - AI შესაძლებელს ხდის მსხვერპლს შესთავაზოს ***პერსონალიზებული პოსტ-კიბერბულინგის მკურნალობა***



MERCY CORPS

როგორ მოვიქცეთ, თუკი შანტაჟის მსხვერპლი გავხდით

როდესაც, ერთი შეხედვით, გამოუვალ მდგომარეობაში ვვარდებით, რთულია იმის დანახვა, თუ როგორ მოქცევა სჯობს. აი, რამდენიმე რჩევა, რომელიც შეიძლება ასეთ სიტუაციაში ყოფნისას გამოგადგეთ:

- **არ ნაშალოთ არაფერი!** შესაძლოა, ეს თქვენი პირველი ინსტინქტი იყოს, მაგრამ ნაშლა არ არის კარგი იდეა. როგორც კი მტკიცებულებების ნაშლას იწყებთ, მოძალადეს უფრო მეტ ძალაუფლებას აძლევთ.

- **არაფერი არ მისცეთ მოძალადეს!** არავითარი დამატებითი ფოტოები თუ მესიჯები, არავითარი პასუხები მის კითხვებზე — საერთოდ არაფერი. არ ეკონტაქტოთ მას.

- **გაუძელით მოლაპარაკების ცდუნებას.** განურჩევლად იმისა, თუ რამდენად უიმედოდ გრძნობთ თავს, მოლაპარაკებას ნუ დაიწყებთ. ეს მოძალადესთან თანამშრომლობის მზაობაზე მეტყველებს.

- **მზად იყავით მოვლენების ყველაზე ცუდი განვითარებისთვის.** იმაზე დაფიქრება, თუ როგორ შეიძლება ინფორმაციის გაჟონვამ იმოქმედოს თქვენზე და რა რეაქცია გექნებათ ამაზე, ისეთი ნაბიჯია, რომელსაც მოძალადეები არ ელიან — ისინი თავიანთ ქმედებებს მხოლოდ თქვენს შიშზე ამყარებენ. ეს სიტუაციაზე ძალაუფლების დაბრუნების ერთ-ერთი გზაა.

- **სირცხვილის გრძნობის გამო დახმარების თხოვნაზე ნუ იტყვით უარს!** თქვენ მარტო არ ხართ — ასეთი რამ შეიძლება ნებისმიერ ადამიანს შეემთხვეს. ესაუბრეთ თქვენს მეგობრებს, ნათესავებს, მასწავლებლებსა თუ თქვენთვის სანდო სხვა პირებს; დაუკავშირდით პოლიციას ან გაესაუბრეთ ადვოკატს.

https://millab.ge/ka/mil-resources/any/28/any/

MERCY CORPS

მდგრადი განვითარების მიზნების ინდიკატორი მეტა-მონაცემები

- მსოფლიო ჯანდაცვის ორგანიზაცია (WHO)
- გაერთიანებული ერეის ბავშვთა ფონდი (UNICEF)
- გაერთიანებული ერების გენდერული თანასწორობის და ქალთა გაძლიერების ბიურო (UN Women)
- გაერთაინებული ერების ნარკოტიკებისა და დანაშაულის ბიურო (UN ODC)
- გაერთიანებული ერების მოსახლეობის ფონდი (UNFPA)
- გაერთიანებული ერების სტატისტიკის განყოფილება (UNSD)

1. გამოდით ანგარიშიდან და აპლიკაციიდან
2. გამოიყენეთ ძლიერი კოდი
3. გადახედეთ ინფორმაციას კონფიდენციალურ ინფორმაციასთან დაკავშირებით
4. მინიმუმამდე დაიყვანეთ ლოკაციის გაზიარება
5. არ ჩაწეროთ ადგილმდებარეობის კოორდინატები სურათებში
6. იზრუნეთ იმაზე, რომ სოციალური მედია ანგარიშები ერთმანეთს დაუკავშიროთ
7. დაუკვირდით, როდესაც იყენებთ უფასო უსადენო ინტერნეტ ქსელებს
8. გამოიყენეთ HTTPS ყველგან
9. გამოიყენეთ ეს მექანიზმები: Use Incognito, Private Browsing, or InPrivate Browsing
10.. გამოიყენეთ ერთზე მეტი ელექტრონული ფოსტის მისამართი

MERCY CORPS

რჩევები, როგორ უზრუნველვყოთ ონლაინ კონფიდენციალობა და უსაფრთხოება

პაროლები

- *საუკეთესო პაროლები* შედგება მინიმუმ 12-15 სიმბოლოსგან და შეიცავს ასოებს, ციფრებს და სიმბოლოებს.
- გამოიყენეთ *სხვადასხვა პაროლები ანგარიშებისთვის*, რომლებიც შეიცავს სენსითიურ ან პირად საიდენტიფიკაციო ინფორმაციას.
- *გადით სისტემიდან, როდესაც დაასრულებთ და უარი თქვით*, როდესაც გკითხავენ, *გსურთ თუ არა მოწყობილობამ*, ბრაუზერმა, საიტმა ან აპმა დაიმახსოვროს თქვენი პაროლი.
- *წაიკითხეთ მეტი პაროლის უსაფრთხოების შესახებ.*

MERCY CORPS

კონფიდენციალობის პარამეტრები და პოლისები

წაიკითხეთ კონფიდენციალურობის პარამეტრების სახელმძღვანელო, რომელსაც ახლა გთავაზობთ ბევრი სოციალური მედიის საიტი და შეცვალეთ თქვენი კონფიდენციალურობის პარამეტრები თქვენი საჭიროებებისდა მიხედვით. აქ მოცემულია რამდენიმე ძირითადი საიტის კონფიდენციალურობის სახელმძღვანელოს ბმული:

- Safety@Facebook
- WhatsApp უსაფრთხოების რჩევები
- ინსტაგრამის უსაფრთხოების ცენტრი
- უსაფრთხოება და კონფიდენციალურობა Twitter-ზე: სახელმძღვანელო შევიწროებისა და შეურაცხყოფის შედეგად გადარჩენილთათვის
- Google უსაფრთხოების ცენტრი
- TikTok უსაფრთხოების ცენტრი
- როგორ ვიყოთ უსაფრთხო Snapchat-ზე

წაიკითხეთ აპებისა და საიტების კონფიდენციალურობის პოლიტიკა, რათა გაარკვიოთ, კიდევ ვის აქვს წვდომა თქვენს ინფორმაციაზე და როგორ შეუძლიათ მიიღონ ისინი. ბევრი საიტი და აპი გააზიარებს ინფორმაციას, თუ ისინი მიიღებენ გამოძახებას ან სასამართლო განკარგულებას, რაც მნიშვნელოვანია ქალებისთვის, რომლებსაც აქვთ ან შეიძლება ჰქონდეთ სასამართლოსთან დაკავშირებული ურთიერთობა იმ პირთან, ვინც მათზე ძალადობდა ან განაგრძობდა მათ დევნას.

წაიკითხეთ მეტი კონფიდენციალურობის მოსაზრებების შესახებ კონტენტის ონლაინ გამოქვეყნებისას.

MERCY CORPS

ჯაშუშური აპლიკაციები

1.FlexiSPY
2.mSpy - არის მობილური და კომპიუტერის მშობელთა კონტროლის მონიტორინგის პროგრამული უზრუნველყოფის ბრენდი iOS, Android, Windows და macOS-ისთვის. აპლიკაცია საშუალებას აძლევს მომხმარებლებს დააკვირდნენ და დაარეგისტრირონ აქტივობა კლიენტის მოწყობილობაზე
3.Spyzie - აკონტროლებს: SMS, ჩეთები, ზარები, GPS - მყისიერად და დისტანციურად თვალთვალის ტელეფონს მისი ნომრის მიხედვით
4.Hoverwatch- mSpy იდეალურად მუშაობს ორივე ოპერაციულ სისტემაზე, ხოლო Hoverwatch ხელმისაწვდომია მხოლოდ Android მოწყობილობებზე
5.Highster Mobile
6.MobileSpy
7.TheTruthSpy
8.XNSPY
9.Spyic
10.Cocospy

MERCY CORPS

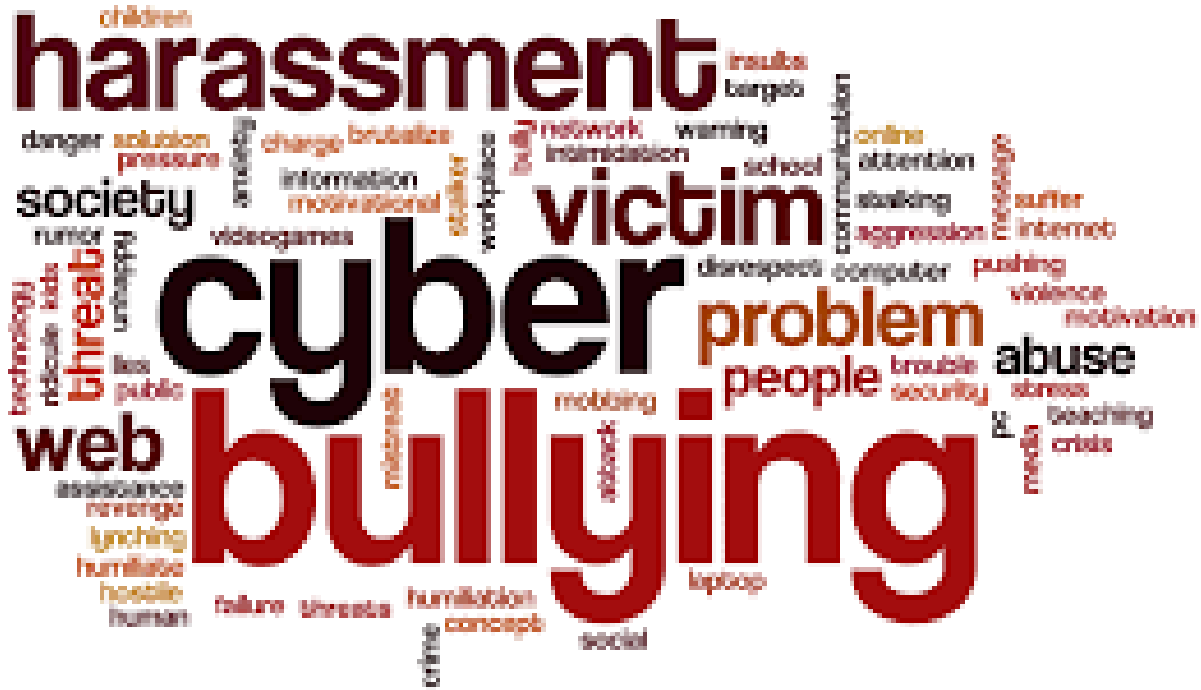
გამოყენებული წყაროები

1. UNFPA, 2021 “Technology-facilitated Gender-based Violence: Making All Spaces Safe”
2. https://www.ictworks.org/technology-facilitated-gender-based-violence/
3. https://digitalrightsfoundation.pk/wp-content/uploads/2020/06/Covid-19.pdf
4. GREVIO (Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence) (2021), *General Recommendation No1 on the digital dimension of violence against women*, Council of Europe, Strasbourg, 20 October 2021 (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).
5. Van der Wilk, A. (2018), Cyber Violence and Hate Speech Online against Women, European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf).
6. 3 Lomba, N., Navarra, C., and Fernandes, M. (2021), Combating Gender-based Violence: Cyber violence – European added value assessment, European Parliamentary Research Service, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf).
7. 4 EIGE (European Institute for Gender Equality) (2020), Gender Equality Index Report, Vilnius https://eige.europa.eu/publications/gender-equality-index-2020-report).
8. 5 GREVIO (Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence) (2021), General Recommendation No1 on the digital dimension of violence against women, Council of Europe, Strasbourg, 20 October 2021 (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).
9. 6 EIGE (2018), Gender equality and digitalization in the European Union, Vilnius (https://eige.europa.eu/publications/gender-equality-and-digitalisation-european-union).
10. https://millab.ge/ka/mil-resources/any/28/any/

MERCY CORPS

11. Georgia: General Policy And Legislation On Cybercrime: Convention on Cybercrime https://police.ge/files/pdf/kiber_danashauli/Cybercrime_Convention_ENG.pdf
12. Armenia: Cybercrime policies/strategies.
13. https://www.coe.int/en/web/octopus/-/armenia
14. Council of Europe: YOUR DIGITAL RIGHTS IN BRIEF. https://rm.coe.int/1680301b6e
15. Internet Freedom and Digital Rights in Georgia: Systemic Challenges.
16. https://idfi.ge/en/internet_freedom_and_digital_rights_in_georgia
17. Internet Freedom in Armenia and Execution of Basic Human Rights in Online Freedom.
18. https://mediainitiatives.am/wp-content/uploads/2018/03/Internet-Freedom-Research-Report-2017-in-English.pdf
19. The internet as a human right.
20. https://www.brookings.edu/articles/the-internet-as-a-human-right/
21. https://www.purchasecommerce.com/blog/ecommerce-security-dimensions
22. https://www.tutorialspoint.com/e_commerce/e_commerce_security.htm
23. https://www.getastra.com/blog/knowledge-base/ecommerce-security/

MERCY CORPS



დიდი მადლობა ყურადღებისთვის!

MERCY CORPS

https://www.youtube.com/watch?v=zLtfoCw16Z0&t=19s