WOMEN AGAINST VIOLENCE EUROPE
WAVE Network and European Info Centre against Violence

Gender Alliance for Development Center
Qendra Aleanca Gjinore për Zhvillim

SIGURIA DIGJITALE ËSHTË SIGURIA E GRAVE

Udhëzues për të njohur dhe për t'u mbrojtur nga dhuna digjitale në marrëdhënie

(Technology-Facilitated Intimate Partner Violence – TF-IPV)

Siguria digjitale është pjesë e sigurisë personale.
Teknologjia duhet të fuqizojë, jo të kontrollojë.

SIGURIA DIGJITALE ËSHTË SIGURIA E GRAVE

Udhëzues për të njohur dhe për t'u mbrojtur nga dhuna digjitale në marrëdhënie *(Technology-Facilitated Intimate Partner Violence – TF-IPV)*

Siguria digjitale është pjesë e sigurisë personale.
Teknologjia duhet të fuqizojë, jo të kontrollojë.

WOMEN AGAINST VIOLENCE EUROPE
WAVE Network and European Info Centre against Violence

Gender Alliance for Development Center
Qendra Aleanca Gjinore për Zhvillim

1. Hyrje

Dhuna në marrëdhënie zakonisht lidhet me forma të dukshme të abuzimit, si dhuna fizike, psikologjike ose ekonomike. Megjithatë, me zhvillimin e teknologjisë dhe përhapjen e gjerë të pajisjeve digjitale, dhuna mund të shfaqet edhe në mënyra më pak të dukshme, përmes mjeteve teknologjike që përdorim çdo ditë.

Telefonat inteligjentë, rrjetet sociale dhe aplikacionet e komunikimit janë bërë pjesë e pandashme e jetës sonë të përditshme. Ato na mundësojnë të qëndrojmë të lidhur me familjen, miqtë dhe kolegët, të ndajmë informacion dhe të komunikojmë në mënyrë të shpejtë dhe të lehtë. Megjithatë, të njëjtat mjete mund të përdoren edhe për qëllime abuzive.

Në disa raste, teknologjia përdoret nga partnerët ose ish-partnerët për të ushtruar kontroll dhe presion mbi një person. Kjo mund të ndodhë përmes kontrollit të telefonit, kërkimit të fjalëkalimeve, monitorimit të aktivitetit në rrjete sociale, ndjekjes së vendndodhjes, dërgimit të mesazheve kërcënuese ose publikimit të materialeve private pa pëlqim.

Kjo formë abuzimi njihet si **dhunë digjitale në marrëdhënie (Technology-Facilitated Intimate Partner Violence – TF-IPV)** dhe i referohet përdorimit të teknologjisë nga partneri ose ish-partneri për të ushtruar kontroll, presion psikologjik, kërcënim apo turpërim ndaj një personi në një marrëdhënie intime. Kjo përfshin përdorimin e teknologjisë për të monitoruar, kontrolluar, kërcënuar ose turpëruar partneren përmes pajisjeve digjitale dhe platformave online.

Dhuna digjitale është një nga format me rritjen më të shpejtë të dhunës ndaj grave dhe vajzave, e cila mund të shkaktojë pasoja reale fizike, psikologjike dhe sociale, si online ashtu edhe offline.

Ndryshe nga format tradicionale të dhunës, ajo mund të ndodhë në çdo moment dhe nga çdo distancë, duke krijuar një ndjenjë të vazhdueshme kontrolli dhe pasigurie për viktimën.

Në shumë raste, dhuna digjitale përdoret për të:

- kontrolluar komunikimet dhe kontaktet e partneres
- monitoruar lëvizjet ose vendndodhjen përmes aplikacioneve ose shërbimeve të lokalizimit
- kërcënuar me publikimin e fotove, videove ose materialeve private
- përhapur informacione poshtëruese ose të pavërteta në rrjete sociale
- ushtruar presion përmes mesazheve të vazhdueshme ose kontrollit të aktivitetit online.

Këto forma abuzimi mund të ndikojnë seriozisht në mirëqenien emocionale, ndjenjën e sigurisë dhe privatësinë e viktimës. Për këtë arsye, është e rëndësishme që dhuna digjitale në marrëdhënie të njihet dhe të trajtohet si një formë reale dhe serioze e dhunës me bazë gjinore.

Dhuna digjitale është një formë reale e dhunës me bazë gjinore dhe duhet të njihet, të parandalohet dhe të trajtohet me të njëjtën seriozitet si format e tjera të dhunës.

Në Shqipëri, përdorimi i internetit dhe rrjeteve sociale është rritur ndjeshëm gjatë viteve të fundit dhe bashkë me të janë shtuar edhe rastet e krimeve kibernetike dhe abuzimeve online. Sipas të dhënave të Policisë së Shtetit, çdo vit regjistrohen qindra kallëzime që lidhen me ndërhyrje në të dhëna kompjuterike, mashtrime online dhe forma të tjera të krimeve kibernetike, duke treguar një rritje të vazhdueshme të këtij fenomeni.
Sipas të dhënave të institucioneve dhe raportimeve në media, rastet e kërcënimeve online, publikimit të materialeve intime dhe përndjekjes në rrjete sociale janë bërë një shqetësim në rritje, veçanërisht për gratë dhe vajzat.
Paralelisht me këto zhvillime, në media dhe në raportet e organizatave të shoqërisë civile janë raportuar edhe raste të abuzimit digjital ndaj grave dhe vajzave, përfshirë kërcënime në rrjete sociale, publikim të materialeve private pa pëlqim dhe përdorim të profileve të rreme për të turpëruar ose përndjekur viktimat. Në disa raste, persona janë hetuar ose arrestuar nga autoritetet për shpërndarje të materialeve intime apo për përdorim të paautorizuar të të dhënave në internet.
Këto zhvillime tregojnë se hapësira digjitale nuk është gjithmonë një mjedis i sigurt dhe se teknologjia mund të përdoret edhe për të ushtruar presion, kontroll ose dhunë në marrëdhënie intime.
Për këtë arsye, është gjithnjë e më e rëndësishme të rritet ndërgjegjësimi për sigurinë digjitale dhe për mënyrat se si mund të identifikohen dhe adresohen format e dhunës digjitale në marrëdhënie.
Ky udhëzues synon të ndihmojë gratë dhe profesionistët të:

- kuptojnë se çfarë është dhuna digjitale në marrëdhënie
- identifikojnë shenjat paralajmëruese të abuzimit
- mësojnë mënyra praktike për të mbrojtur sigurinë e tyre digjitale
- dinë ku dhe si të kërkojnë ndihmë në rast abuzimi.

Udhëzuesi synon gjithashtu të rrisë ndërgjegjësimin mbi rëndësinë e privatësisë dhe sigurisë në hapësirën digjitale.

2. Çfarë është dhuna digjitale në marrëdhënie?

Dhuna digjitale në marrëdhënie është një formë e dhunës që realizohet përmes përdorimit të teknologjisë. Ajo përfshin çdo formë **kontrolli, manipulimi, kërcënimi ose përndjekjeje që kryhet përmes pajisjeve digjitale dhe platformave online**.

Kjo formë dhune ndodh kur teknologjia përdoret nga partneri ose ish-partneri për të kufizuar lirinë, privatësinë ose sigurinë e një personi në një marrëdhënie intime. Ndryshe nga disa forma të tjera të dhunës që ndodhin në hapësira fizike, dhuna digjitale mund të ndodhë në çdo kohë dhe nga çdo distancë, duke e bërë viktimën të ndihet e monitoruar ose e kontrolluar vazhdimisht.

Teknologjia mund të përdoret për të ushtruar kontroll dhe presion në mënyra të ndryshme. Për shembull, një partner mund të kërkojë fjalëkalimet e rrjeteve sociale, të kontrollojë mesazhet private, të monitorojë vendndodhjen përmes aplikacioneve ose të dërgojë vazhdimisht mesazhe për të kërkuar përgjigje dhe për të ushtruar presion emocional.
Në disa raste, këto sjellje mund të paraqiten si shenja kujdesi, xhelozie ose interesimi, por kur ato bëhen të vazhdueshme dhe kufizojnë lirinë e një personi, ato mund të përbëjnë forma të dhunës digjitale. Sjellje të tilla shpesh shfaqen gradualisht dhe mund të jenë të vështira për t'u identifikuar në fillim, veçanërisht kur paraqiten si shqetësim ose interesim për partneren.

Dhuna digjitale mund të përdoret për të:

- **kontrolluar komunikimet dhe kontaktet** – për shembull duke kërkuar qasje në telefon, email ose rrjete sociale dhe duke kontrolluar me kë komunikon partnerja
- **monitoruar vendndodhjen ose aktivitetin online** – përmes aplikacioneve të lokalizimit, ndarjes së vendndodhjes ose kontrollit të aktivitetit në rrjete sociale
- **turpëruar ose dëmtuar reputacionin në internet** – përmes publikimit të komenteve poshtëruese, përhapjes së informacioneve të pavërteta ose përdorimit të profileve të rreme
- **kërcënuar me publikimin e materialeve private** – si fotografi, video ose mesazhe personale, të cilat mund të përdoren për shantazh ose presion
- **ushtruar presion psikologjik përmes komunikimeve të vazhdueshme** – për shembull duke dërguar një numër të madh mesazhesh, duke kërkuar përgjigje të menjëhershme ose duke reaguar me zemërim nëse komunikimi nuk ndodh sipas pritshmërive.

Në shumë raste, dhuna digjitale nuk ndodh e izoluar. Ajo shpesh shoqërohet me forma të tjera të dhunës dhe kontrollit në marrëdhënie, si:

- **dhuna psikologjike**, përmes kërcënimeve, manipulimit dhe presionit emocional
- **manipulimi emocional**, ku teknologjia përdoret për të krijuar ndjenja faji, frike ose varësie
- **dhuna fizike**, ku kontrolli digjital shoqërohet me forma të tjera të abuzimit
- **kontrolli ekonomik**, për shembull duke monitoruar ose kufizuar aksesin në burime financiare përmes pajisjeve ose aplikacioneve.

Kombinimi i këtyre formave të kontrollit mund ta bëjë viktimën të ndihet e izoluar, e frikësuar dhe e paaftë për të kërkuar ndihmë.
Një nga sfidat kryesore të kësaj forme dhune është se ajo mund të jetë më e vështirë për t'u identifikuar. Sjellje të tilla si kontrolli i telefonit ose kërkesa për fjalëkalime shpesh mund të justifikohen si shenja kujdesi ose xhelozie, ndërsa në fakt mund të jenë tregues të një modeli kontrolli dhe abuzimi.
Për më tepër, teknologjia mund ta bëjë këtë formë dhune të vazhdueshme. Ndryshe nga dhuna që ndodh vetëm në hapësira fizike, dhuna digjitale mund të vazhdojë edhe kur personat nuk janë

pranë njëri-tjetrit, duke krijuar një ndjenjë të përhershme presioni, frike dhe pasigurie për viktimën.

Prandaj është e rëndësishme që dhuna digjitale në marrëdhënie të njihet dhe të kuptohet si një formë serioze e dhunës me bazë gjinore, e cila kërkon vëmendje, ndërgjegjësim dhe mekanizma mbështetjeje për viktimat.

3. Si ndodh dhuna digjitale?

Dhuna digjitale mund të shfaqet në forma të ndryshme dhe shpesh ndodh përmes mjeteve që përdorim çdo ditë.

Kontrolli i telefonit

Një nga format më të zakonshme të dhunës digjitale është kontrolli i pajisjeve personale.
Kjo mund të përfshijë:

- kërkimin e fjalëkalimeve të telefonit ose rrjeteve sociale
- kontrollimin e mesazheve dhe historikut të komunikimeve
- leximin e email-eve ose mesazheve private
- instalimin e aplikacioneve që monitorojnë aktivitetin në telefon,
    - si *Find My* (Apple), *Google Find My Device* ose *Life360*, të cilat mund të tregojnë në kohë reale vendndodhjen e një personi,
    - *Google Family Link* ose *Qustodio*, që lejojnë monitorimin e përdorimit të telefonit, aplikacioneve dhe aktivitetit online.
    - **mSpy** ose **FlexiSPY**, që mund të përdoren për të monitoruar mesazhet, telefonatat dhe aktivitetin në pajisje.
    - **KidsGuard** ose **Hoverwatch**, që ofrojnë funksione për gjurmimin e aktivitetit në telefon dhe përdorimin e aplikacioneve.
    - **Spyic** ose **Cocospy**, që pretendojnë të monitorojnë përdorimin e pajisjes, kontaktet dhe historikun e aktivitetit online.
    - **uMobix** ose **Spyzie**, që mund të përdoren për të ndjekur aktivitetin në disa rrjete sociale dhe aplikacione mesazhesh.
- Këto forma përfshijnë gjithashtu shantazhin seksual (sextortion), manipulimin e imazheve (p.sh. deepfake), dhe përdorimin e teknologjive për ndjekje dhe survejim.

Edhe pse shumë nga këto aplikacione janë krijuar për qëllime legjitime, si siguria e familjes ose gjetja e pajisjeve të humbura, ato mund të keqpërdoren në marrëdhënie për të monitoruar dhe kontrolluar partnerin pa dijeninë ose pëlqimin e tij/saj.

Ndjekja online (stalking digjital)

Ndjekja online ndodh kur një person përdor teknologjinë për të monitoruar vazhdimisht aktivitetin, komunikimet ose vendndodhjen e partneres. Kjo formë kontrolli mund të krijojë një ndjenjë të vazhdueshme presioni dhe pasigurie, pasi viktima mund të ndihet e vëzhguar ose e kontrolluar në çdo moment.
Ndjekja digjitale mund të realizohet përmes mjeteve dhe platformave që përdoren çdo ditë, duke e bërë shpesh të vështirë për t'u identifikuar.
Kjo mund të përfshijë:

- përdorimin e aplikacioneve për gjurmim të vendndodhjes për të parë në kohë reale ku ndodhet partnerja
- kontrollimin e vazhdueshëm të aktivitetit në rrjete sociale, si postimet, komentet, "likes" ose personat me të cilët ndërvepron
- monitorimin e kontakteve dhe komunikimeve për të zbuluar me kë flet ose shkëmben mesazhe
- përdorimin e profileve të rreme ose llogarive të tjera për të ndjekur aktivitetin online të partneres pa dijeninë e saj.

Shpërndarja e materialeve private

Një nga format më serioze të dhunës digjitale në marrëdhënie është shpërndarja ose kërcënimi për publikimin e materialeve private. Kjo ndodh kur një person përdor fotografi, video ose komunikime personale për të ushtruar presion, kontroll ose për të turpëruar partneren.

Në shumë raste, këto materiale janë ndarë fillimisht në mënyrë private brenda marrëdhënies, por më pas përdoren si mjet manipulimi ose shantazhi.
Kjo mund të përfshijë:

- publikimin e fotove ose videove intime pa pëlqimin e personit
- kërcënimin për publikimin e materialeve personale në rrjete sociale ose platforma të tjera online
- dërgimin e materialeve private tek miqtë, familjarët ose kolegët për të dëmtuar reputacionin e viktimës
- përdorimin e përmbajtjeve private për shantazh ose për të ushtruar presion që viktima të bëjë diçka kundër vullnetit të saj.

Kjo formë abuzimi mund të ketë pasoja të rënda psikologjike dhe sociale për viktimën, duke ndikuar në privatësinë, reputacionin dhe ndjenjën e sigurisë së saj.

Ngacmimi dhe kërcënimi online

Abuzimi digjital mund të ndodhë edhe përmes komunikimeve të vazhdueshme ose kërcënuese në internet. Në këto raste, teknologjia përdoret për të ushtruar presion psikologjik, për të frikësuar ose për të turpëruar një person përmes mesazheve dhe ndërveprimeve online.

Kjo formë abuzimi mund të ndodhë përmes rrjeteve sociale, aplikacioneve të mesazheve, email-it ose platformave të tjera të komunikimit dhe shpesh karakterizohet nga komunikime të përsëritura dhe agresive.

Kjo përfshin:

- dërgimin e mesazheve kërcënuese ose frikësuese përmes aplikacioneve të mesazheve ose rrjeteve sociale
- publikimin e komenteve poshtëruese, fyese ose denigruese në rrjete sociale
- dërgimin e vazhdueshëm të mesazheve për të ushtruar presion, për të kërkuar përgjigje të menjëhershme ose për të kontrolluar komunikimin
- përhapjen e komenteve ose informacioneve që synojnë të turpërojnë ose të dëmtojnë reputacionin e viktimës.

Këto forma komunikimi mund të krijojnë ndjenja frike, ankthi dhe presioni të vazhdueshëm për personin që i përjeton.

4. Shenja paralajmëruese

Dhuna digjitale në marrëdhënie shpesh nuk fillon menjëherë me kërcënime apo abuzim të hapur. Në shumë raste, ajo nis me sjellje që mund të duken si shenja xhelozie, kujdesi ose interesimi për partneren. Megjithatë, me kalimin e kohës këto sjellje mund të shndërrohen në forma të qarta kontrolli dhe abuzimi.

Kontrolli i vazhdueshëm i komunikimeve, kërkesa për akses në llogaritë personale ose monitorimi i aktivitetit online mund të jenë tregues të hershëm të dhunës digjitale. Këto sjellje shpesh synojnë të kufizojnë privatësinë dhe lirinë e personit dhe mund të krijojnë ndjenja presioni, frike ose pasigurie.

Mund të jeni duke përjetuar dhunë digjitale nëse partneri:

- kërkon të dijë vazhdimisht ku ndodheni dhe kërkon të ndani vendndodhjen tuaj në çdo moment
- kërkon fjalëkalimet e rrjeteve sociale, email-it ose telefonit tuaj
- zemërohet ose bëhet agresiv nëse nuk përgjigjeni menjëherë në mesazhe ose telefonata
- kontrollon telefonin, mesazhet ose rrjetet sociale pa lejen tuaj

- monitoron aktivitetin tuaj online, si postimet, komentet ose personat me të cilët ndërveproni
- kërkon të dijë me kë komunikoni dhe për çfarë flisni
- ju dërgon vazhdimisht mesazhe për të kontrolluar aktivitetin tuaj gjatë ditës
- ju kritikon ose ju turpëron për mënyrën si përdorni rrjetet sociale
- ju kërcënon me publikimin e mesazheve, fotove ose videove private.

Nëse këto sjellje ndodhin shpesh dhe krijojnë ndjenja presioni, frike ose kontrolli, ato mund të jenë tregues të dhunës digjitale në marrëdhënie.

Njohja e këtyre shenjave është një hap i rëndësishëm për të kuptuar kur një marrëdhënie mund të jetë duke u bërë abuzive dhe për të kërkuar mbështetje në kohën e duhur.

5. Si mund të mbroheni

Siguria digjitale është një pjesë e rëndësishme e sigurisë personale. Disa masa të thjeshta mund të ndihmojnë në mbrojtjen e privatësisë dhe në reduktimin e rrezikut nga monitorimi ose abuzimi online. Këto masa lidhen me atë që njihet si "higjienë kibernetike", që përfshin praktikat e përditshme për të mbrojtur pajisjet, të dhënat dhe privatësinë në hapësirën digjitale. Është e rëndësishme të jeni të vetëdijshëm për mënyrën se si përdorni pajisjet dhe llogaritë tuaja digjitale, si dhe të kontrolloni rregullisht cilësimet e sigurisë.

Siguroni llogaritë tuaja

Llogaritë digjitale, si rrjetet sociale, email-i apo aplikacionet e komunikimit, përmbajnë shumë informacion personal. Mbrojtja e tyre është një hap i rëndësishëm për të ruajtur privatësinë dhe për të parandaluar aksesin e paautorizuar.

- përdorni fjalëkalime të forta dhe të ndryshme për çdo llogari, duke shmangur përdorimin e të njëjtit fjalëkalim në disa platforma
- aktivizoni verifikimin me dy hapa (Two-Factor Authentication – 2FA) për të shtuar një shtresë shtesë sigurie në llogaritë tuaja
- mos ndani fjalëkalimet me askënd dhe shmangni ruajtjen e tyre në vende që mund të aksesohen lehtësisht nga të tjerët
- ndryshoni rregullisht fjalëkalimet, veçanërisht nëse dyshoni se dikush tjetër mund të ketë akses në llogaritë tuaja.

Kontrolloni privatësinë në rrjete sociale

Rrjetet sociale shpesh përmbajnë informacion të detajuar për jetën personale, vendndodhjen dhe aktivitetin e përditshëm. Rishikimi i cilësimeve të privatësisë mund të ndihmojë në kufizimin e aksesit të personave të tjerë në këtë informacion.

- rishikoni dhe përditësoni rregullisht cilësimet e privatësisë në rrjete sociale

• kufizoni informacionin personal që publikoni online, si vendndodhja, planet e udhëtimit ose detaje të jetës private
• kontrolloni se kush mund të shohë postimet, fotot dhe informacionin personal në profilin tuaj
• jini të kujdesshëm me kërkesat për miqësi nga persona të panjohur ose profile të dyshimta.

Kontrolloni aplikacionet në telefon

Telefonat inteligjentë mund të përmbajnë shumë aplikacione që kanë akses në informacione personale si vendndodhja, kontaktet ose kamera. Kontrollimi i këtyre aplikacioneve është një hap i rëndësishëm për të mbrojtur privatësinë tuaj.

• kontrolloni rregullisht nëse në telefon ka aplikacione që nuk i keni instaluar vetë
• shikoni cilat aplikacione kanë akses në vendndodhje, kamera, mikrofon ose kontakte
• kontrolloni rregullisht nëse vendndodhja juaj po ndahet përmes aplikacioneve si Google Maps, Find My ose WhatsApp
• çaktivizoni ndarjen e vendndodhjes kur nuk është e nevojshme
• përditësoni rregullisht sistemin dhe aplikacionet për të rritur sigurinë e pajisjes.

Ruani provat

Nëse përjetoni abuzim digjital, ruajtja e provave mund të jetë e rëndësishme nëse vendosni të raportoni rastin ose të kërkoni ndihmë.

• bëni screenshot të mesazheve kërcënuese ose abuzive
• ruani email-et, mesazhet dhe komunikimet që përmbajnë kërcënime ose presion
• mbani shënim datat, orët dhe situatat kur ndodhin kërcënimet ose abuzimi
• nëse është e mundur, ruani kopje të provave në një vend të sigurt ose në një pajisje tjetër.

Marrja e këtyre hapave mund të ndihmojë në mbrojtjen e sigurisë dhe privatësisë suaj digjitale dhe në krijimin e një mjedisi më të sigurt online.

6. Çfarë të bëni nëse përjetoni dhunë digjitale

Nëse dyshoni se jeni duke përjetuar dhunë digjitale në marrëdhënie, është e rëndësishme të dini se nuk jeni vetëm dhe se ekzistojnë mënyra për të kërkuar ndihmë dhe për të mbrojtur veten. Dhuna digjitale shpesh mbetet e pa-raportuar për shkak të mungesës së mekanizmave, frikës nga pasojat dhe mungesës së besimit tek institucionet. Marrja e disa hapave të kujdesshëm mund të ndihmojë në mbrojtjen e sigurisë suaj dhe në adresimin e situatës.

I. **Mos e përballoni situatën vetëm**
Dhuna digjitale mund të krijojë ndjenja izolimi, frike ose presioni. Megjithatë, është e rëndësishme të kërkoni mbështetje. Flisni me dikë që i besoni dhe që mund t'ju mbështesë emocionalisht dhe praktikisht.

II. **Ruani çdo provë të komunikimeve abuzive**
Nëse merrni mesazhe kërcënuese ose përjetoni forma të tjera abuzimi online, përpiquni të ruani provat. Kjo mund të përfshijë screenshot të mesazheve, email-eve ose postimeve në rrjete sociale. Këto prova mund të jenë të rëndësishme nëse vendosni të raportoni rastin.

III. **Flisni me një person të besuar ose profesionist**
Mund të jetë e dobishme të ndani përvojën tuaj me një mik, familjar, këshilltar ose profesionist që punon me viktimat e dhunës. Organizatat e shoqërisë civile dhe shërbimet e mbështetjes për viktimat mund të ofrojnë informacion, këshillim dhe orientim për hapat e mëtejshëm.

IV. **Raportoni abuzimin në platformën ku ndodh**
Shumica e rrjeteve sociale dhe platformave të komunikimit kanë mekanizma për raportimin e abuzimit ose kërcënimeve. Raportimi i përmbajtjes abuzive mund të ndihmojë në heqjen e saj dhe në kufizimin e sjelljes së personit që ushtron abuzim.

V. **Kontaktoni autoritetet në rast kërcënimesh serioze**
Nëse kërcënimet janë serioze ose nëse ndiheni në rrezik, kontaktoni autoritetet përkatëse. Institucionet e zbatimit të ligjit mund të ndërhyjnë dhe të trajtojnë rastet e kërcënimeve, shantazhit ose shpërndarjes së materialeve private.

VI. Në rastet kur përfshihen materiale intime të shpërndara pa pëlqim, ekzistojnë edhe mjete teknike që ndihmojnë në kufizimin e përhapjes së tyre, si StopNCII[1], i cili mbështet parandalimin e rishpërndarjes së përmbajtjes online.

Marrja e këtyre hapave mund të ndihmojë në mbrojtjen e sigurisë dhe privatësisë suaj. Kujtoni se dhuna digjitale është një formë reale e dhunës dhe se kërkimi i ndihmës është një hap i rëndësishëm drejt mbrojtjes së vetes dhe të drejtave tuaja.

7. Ku mund të kërkoni ndihmë në Shqipëri

Nëse përjetoni dhunë digjitale në marrëdhënie ose ndiheni të kërcënuar përmes teknologjisë, është e rëndësishme të dini se ekzistojnë institucione dhe organizata që mund të ofrojnë mbështetje. Këto struktura mund t'ju ndihmojnë me informacion, këshillim, mbështetje ligjore dhe ndërhyrje në rastet e abuzimit.

Policia e Shtetit

[1] https://stopncii.org/

Në rastet kur përballeni me kërcënime serioze, shantazh, përndjekje ose publikim të materialeve private pa pëlqimin tuaj, mund të kontaktoni Policinë e Shtetit.

Numri emergjencave: 129

Policia mund të ndërhyjë në rastet kur siguria juaj është në rrezik dhe mund të nisë procedura ligjore në rastet e dhunës, kërcënimeve ose krimeve kibernetike.

Raportimi i krimeve kibernetike

Rastet që lidhen me abuzimin online, ndërhyrjen në të dhëna, shpërndarjen e materialeve private ose forma të tjera të krimeve digjitale mund të raportohen pranë Njësisë për Hetimin e Krimeve Kompjuterike në Policinë e Shtetit.
Kjo njësi merret me hetimin e krimeve që ndodhin në hapësirën digjitale dhe mund të ofrojë mbështetje në rastet e abuzimit përmes teknologjisë.

Linja Kombëtare e Këshillimit për Gra dhe Vajza[2]

Gratë dhe vajzat që përjetojnë dhunë mund të kërkojnë mbështetje përmes Linjës Kombëtare të Këshillimit për Gra dhe Vajza, e cila ofron këshillim dhe informacion falas.

Telefon: 116 117

Përmes kësaj linje mund të merrni këshillim profesional, informacion mbi të drejtat tuaja dhe orientim drejt shërbimeve të tjera mbështetëse.

iSIGURT.al – Platforma Kombëtare për Internet të Sigurt në Shqipëri

iSIGURT.al[3] është një mekanizëm kombëtar për raportimin e incidenteve online, përfshirë bullizmin, dhunën digjitale, përmbajtjet e papërshtatshme dhe gjuhën e urrejtjes. Platforma shërben gjithashtu si burim informacioni dhe udhëzimi për përdorimin e sigurt të internetit nga fëmijët, të rinjtë dhe të rriturit, si dhe për profesionistët që punojnë me ta.

Aplikacioni The Sorority – Bashkë. Tani. Kudo.[4]

Aplikacione komunitare sigurie, si "The Sorority – Bashkë. Tani. Kudo.", janë platforma digjitale të krijuara për të rritur sigurinë personale përmes mbështetjes së komunitetit. Ato u mundësojnë përdorueseve të aktivizojnë një alarm sigurie, të ndajnë vendndodhjen dhe të kërkojnë ndihmë nga persona të besuar ose anëtarë të tjerë të komunitetit në afërsi, në situata pasigurie.

---

[2] https://hotlinealbania.org/?fbclid=IwY2xjawRcBghleHRuA2FlbQIxMABicmlkETF2SUVsbUV5T28wZEhCWXZ4c3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHt-3T2juyz1wHEIcmzMF24Km82V1-K5vE26ntYpEZXAl5WBBzt7Mi0K3vSzQ_aem_RVbwIxI_6rxhF1oR9vjQtA

[3] https://isigurt.al/

[4] https://www.jointhesorority.com/?lang=en

Organizatat e shoqërisë civile

Në Shqipëri veprojnë një sërë organizatash që punojnë për mbrojtjen e të drejtave të grave dhe për mbështetjen e viktimave të dhunës. Këto organizata mund të ofrojnë shërbime të ndryshme mbështetëse, si:

- këshillim psikologjik për viktimat e dhunës
- mbështetje dhe këshillim ligjor
- informacion mbi të drejtat dhe procedurat e raportimit
- orientim drejt institucioneve dhe shërbimeve përkatëse.

Rrjete kombëtare si Albanian Women Empowerment Network (AWEN)[5] punojnë për mbrojtjen e të drejtave të grave dhe adresimin e dhunës me bazë gjinore, përfshirë edhe format që shfaqen në hapësirat digjitale, përmes ndërgjegjësimit, advokimit dhe forcimit të kapaciteteve të institucioneve dhe organizatave.

Organizata dhe iniciativa si SCiDEV[6] kontribuojnë në rritjen e ndërgjegjësimit për sigurinë digjitale, të drejtat online dhe forcimin e reziliencës kibernetike të mediave dhe organizatave të shoqërisë civile.

Kërkimi i ndihmës është një hap i rëndësishëm për të mbrojtur sigurinë dhe mirëqenien tuaj. Nëse përjetoni dhunë digjitale, mos hezitoni të kontaktoni një nga këto struktura për mbështetje dhe informacion.

8. 11 hapa për të rritur sigurinë digjitale

Siguria digjitale fillon me disa masa të thjeshta që mund të aplikohen në përdorimin e përditshëm të telefonit, kompjuterit dhe rrjeteve sociale. Këta hapa mund t'ju ndihmojnë të mbroheni më mirë nga monitorimi, abuzimi ose akseset e paautorizuara në llogaritë dhe pajisjet tuaja.

I. **Mos ndani fjalëkalimet me askënd.**
Fjalëkalimet janë çelësi i sigurisë së llogarive tuaja dhe duhet të mbahen gjithmonë private.

II. **Aktivizoni verifikimin me dy hapa (2FA).**
Kjo shton një shtresë shtesë sigurie duke kërkuar një kod verifikimi përveç fjalëkalimit.

III. **Kontrolloni dhe përditësoni cilësimet e privatësisë në rrjetet sociale.**
Sigurohuni që vetëm personat që dëshironi të kenë akses në informacionin dhe postimet tuaja.

IV. **Kufizoni informacionin personal që publikoni online.**

[5] https://www.awenetwork.org/
[6] https://scidevcenter.org/

Shmangni ndarjen e detajeve të ndjeshme si vendndodhja, planet e udhëtimit ose informacione personale.

V. **Kontrolloni aplikacionet që kanë akses në vendndodhjen tuaj.**
Çaktivizoni aksesin për aplikacionet që nuk kanë nevojë për këtë informacion.

VI. **Mos klikoni në linke ose mesazhe të dyshimta.**
Linket e panjohura mund të përdoren për mashtrim ose për të marrë akses në të dhënat tuaja.

VII. **Përditësoni rregullisht aplikacionet dhe sistemin e telefonit.**
Përditësimet shpesh përmbajnë përmirësime të sigurisë që mbrojnë pajisjen tuaj.

VIII. **Bëni kopje rezervë të të dhënave të rëndësishme.**
Ruani informacionin e rëndësishëm në një vend të sigurt, si një cloud i besueshëm ose pajisje tjetër.

IX. **Ruani provat në rast abuzimi online.**
Screenshot-et dhe komunikimet e ruajtura mund të jenë të rëndësishme nëse vendosni të raportoni një rast.

X. **Kërkoni ndihmë nëse ndiheni të pasigurt.**
Kontaktoni një person të besuar, një organizatë mbështetëse ose autoritetet nëse përjetoni dhunë digjitale.

XI. Dilni nga llogaritë tuaja në pajisje që përdoren nga persona të tjerë.

Këta hapa mund të ndihmojnë në krijimin e një mjedisi më të sigurt për përdorimin e teknologjisë dhe në mbrojtjen e privatësisë dhe sigurisë suaj digjitale.

9. A mund të jetë telefoni juaj duke u monitoruar?

6 shenja paralajmëruese

Në disa raste, aplikacione ose mjete të tjera digjitale mund të përdoren për të monitoruar aktivitetin në telefon pa dijeninë e përdoruesit. Kjo mund të përfshijë gjurmimin e vendndodhjes, kontrollin e mesazheve ose monitorimin e aktivitetit në internet. Nëse dyshoni për një situatë të tillë, është e rëndësishme të jeni të vetëdijshëm për disa shenja paralajmëruese.

1. **Bateria e telefonit shkarkohet shumë shpejt**
   Nëse bateria e telefonit fillon të mbarojë shumë më shpejt se zakonisht, kjo mund të jetë një shenjë që disa aplikacione po funksionojnë vazhdimisht në sfond për të mbledhur ose transmetuar të dhëna.
2. **Telefoni nxehet edhe kur nuk është në përdorim**
   Nëse telefoni nxehet shpesh pa ndonjë arsye të qartë, mund të jetë një tregues që disa aplikacione po punojnë në sfond dhe po përdorin burimet e pajisjes.
3. **Ka aplikacione që nuk i keni instaluar vetë**

Kontrolloni listën e aplikacioneve në telefon. Nëse shihni aplikacione që nuk i mbani mend t'i keni instaluar, është e rëndësishme të verifikoni funksionin e tyre dhe nëse kanë akses në informacion personal.

4. **Përdorim i pazakontë i internetit ose i të dhënave mobile**
   Nëse përdorimi i internetit rritet ndjeshëm pa ndonjë arsye të dukshme, mund të jetë një shenjë që një aplikacion po dërgon të dhëna nga pajisja juaj.
5. **Telefoni sillet në mënyrë të pazakontë**
   Rinisje të papritura, hapje automatike e aplikacioneve ose dërgim i mesazheve pa dijeninë tuaj mund të jenë sinjale që pajisja nuk po funksionon normalisht.
6. **Partneri duket se di shumë për aktivitetin tuaj digjital**
   Nëse një person duket se di detaje për vendndodhjen tuaj, komunikimet ose aktivitetin online pa ia treguar ju, kjo mund të jetë një shenjë që informacioni po monitorohet.

Në disa raste, këto shenja mund të kenë edhe shpjegime teknike normale, por nëse ndodhin njëkohësisht me sjellje kontrolluese nga partneri, është e rëndësishme të kërkoni këshillë dhe mbështetje nga një profesionist i teknologjisë ose nga organizata që ofrojnë mbështetje për viktimat e dhunës digjitale. Kontrollimi i pajisjes dhe marrja e masave për rritjen e sigurisë digjitale mund të ndihmojë në mbrojtjen e privatësisë dhe sigurisë suaj.

9.1 Si të kontrolloni nëse vendndodhja juaj po ndahet

Në shumë raste, aplikacionet në telefon mund të ndajnë automatikisht vendndodhjen tuaj me persona të tjerë ose me aplikacione të caktuara. Kontrollimi i këtyre cilësimeve mund të ndihmojë në mbrojtjen e privatësisë suaj.

Kontrolloni ndarjen e vendndodhjes në telefon

Në telefonat Android ose iPhone mund të kontrolloni cilat aplikacione kanë akses në vendndodhjen tuaj.

Në iPhone:

- Settings
- Privacy & Security
- Location Services
- shikoni cilat aplikacione kanë akses në vendndodhjen tuaj

Në Android:

- Settings
- Location
- App location permissions
- kontrolloni cilat aplikacione mund të përdorin vendndodhjen tuaj

Nëse shihni aplikacione që nuk i përdorni ose nuk i njihni, mund të çaktivizoni aksesin e tyre në vendndodhje.

Kontrolloni nëse vendndodhja ndahet me persona të tjerë

Disa aplikacione lejojnë ndarjen e vendndodhjes në kohë reale me persona të tjerë.
Kontrolloni veçanërisht:

- Google Maps (Location sharing)
- Find My (Apple)
- WhatsApp (Live Location)
- Life360

Sigurohuni që vendndodhja juaj të mos jetë duke u ndarë me persona pa dijeninë tuaj.

Çaktivizoni ndarjen e vendndodhjes në WhatsApp

Në WhatsApp mund të ndani vendndodhjen në kohë reale me persona të tjerë përmes funksionit **Live Location**.
Për të kontrolluar nëse vendndodhja juaj po ndahet:
• hapni WhatsApp
• shkoni në bisedën ku mund të jetë ndarë vendndodhja
• kontrolloni nëse është aktiv funksioni **Live Location**
• nëse është aktiv, zgjidhni **Stop sharing** për ta ndaluar ndarjen e vendndodhjes.

Kontrolloni ndarjen e vendndodhjes në rrjete sociale

Disa rrjete sociale mund të tregojnë vendndodhjen në postime ose në foto.
Është e rekomandueshme të:

- mos publikoni vendndodhjen në kohë reale
- çaktivizoni vendndodhjen automatike në foto
- kontrolloni cilësimet e privatësisë në aplikacionet sociale

10. Checklist: Siguria Digjitale

Ky checklist mund t'ju ndihmojë të vlerësoni nëse po merrni disa nga hapat bazë për të mbrojtur sigurinë dhe privatësinë tuaj digjitale. Kontrolloni nëse këto masa sigurie janë aktive në pajisjet dhe llogaritë tuaja:

☐ Përdor **fjalëkalime të forta dhe të ndryshme për çdo llogari** digjitale

☐ Kam **aktivizuar verifikimin me dy hapa (2FA)** në llogaritë e rëndësishme si email, rrjete sociale dhe aplikacione komunikimi

☐ **Kontrolloj rregullisht cilësimet e privatësisë** në rrjetet sociale dhe kufizoj informacionin që është publik

☐ **Nuk ndaj fjalëkalimet ose kodet e verifikimit** me askënd

☐ **Kontrolloj aplikacionet e instaluara në telefon** dhe heq ato që nuk i përdor ose nuk i njoh

☐ **Kontrolloj cilat aplikacione kanë akses në vendndodhje, kamera ose mikrofon**

☐ **Ruaj provat në rast abuzimi online**, si mesazhe, email-e ose postime kërcënuese

☐ **Di ku të kërkoj ndihmë** dhe cilat institucione ose organizata mund të më mbështesin në rast dhune digjitale.

☐ **Kontrolloj rregullisht nëse vendndodhja ime po ndahet me aplikacione ose persona të tjerë**

Ky checklist mund të përdoret si një udhëzues i thjeshtë për të forcuar sigurinë tuaj digjitale dhe për të identifikuar nëse ka hapa të tjerë që mund të ndërmerrni për të mbrojtur privatësinë dhe sigurinë tuaj online.

11. Udhëzues për profesionistët dhe organizatat

Profesionistët dhe organizatat që punojnë me viktimat e dhunës me bazë gjinore luajnë një rol të rëndësishëm në identifikimin dhe adresimin e dhunës digjitale në marrëdhënie. Duke qenë se teknologjia është bërë pjesë e përditshme e jetës, është e rëndësishme që siguria digjitale të konsiderohet si një element i rëndësishëm gjatë vlerësimit dhe mbështetjes së rasteve të dhunës.

Profesionistët që punojnë në shërbimet sociale, organizatat e shoqërisë civile, institucionet publike apo në sektorin e drejtësisë mund të ndihmojnë në rritjen e ndërgjegjësimit dhe në ofrimin e mbështetjes për viktimat që përjetojnë forma të abuzimit digjital.

Rekomandohet që profesionistët:

- të përfshijnë **sigurinë digjitale si pjesë të vlerësimit të rasteve**, duke pyetur nëse viktima përjeton kontroll ose monitorim përmes teknologjisë
- të ndihmojnë viktimat **të kuptojnë rreziqet që lidhen me përdorimin e teknologjisë dhe rrjeteve sociale**
- të ofrojnë **informacion praktik për mbrojtjen e llogarive, pajisjeve dhe privatësisë online**
- të ndihmojnë viktimat në **dokumentimin dhe ruajtjen e provave të abuzimit digjital**
- të bashkëpunojnë me **institucionet përkatëse dhe strukturat e zbatimit të ligjit** në rastet kur kërkohet raportimi ose ndërhyrja institucionale
- të referojnë viktimat drejt **shërbimeve të specializuara për mbështetje psikologjike, ligjore ose sociale**.

Adresimi i dhunës digjitale kërkon jo vetëm mbështetje për viktimat, por edhe përgjegjësi nga institucionet dhe platformat digjitale për parandalim dhe reagim efektiv.

Rritja e ndërgjegjësimit për dhunën digjitale dhe integrimi i sigurisë digjitale në shërbimet e mbështetjes për viktimat janë hapa të rëndësishëm për të garantuar që hapësira digjitale të jetë më e sigurt për gratë dhe vajzat. Përmes bashkëpunimit ndërmjet institucioneve, organizatave dhe profesionistëve, mund të krijohen mekanizma më efektivë për parandalimin dhe adresimin e kësaj forme dhune.

12. Përfundime

Dhuna digjitale në marrëdhënie është një formë gjithnjë e më e dukshme e dhunës me bazë gjinore, e cila shfaqet përmes përdorimit të teknologjisë për të kontrolluar, kërcënuar ose përndjekur partneren. Edhe pse ndodh në hapësirën online, pasojat e saj janë shumë reale dhe mund të ndikojnë ndjeshëm në mirëqenien emocionale, sigurinë dhe privatësinë e viktimës.

Përhapja e teknologjisë dhe përdorimi i gjerë i rrjeteve sociale kanë krijuar mundësi të reja për komunikim dhe lidhje, por njëkohësisht kanë sjellë edhe sfida të reja në lidhje me sigurinë dhe mbrojtjen e privatësisë. Në këtë kontekst, është e rëndësishme që dhuna digjitale të njihet, të kuptohet dhe të trajtohet si një formë serioze e abuzimit në marrëdhënie.

Rritja e ndërgjegjësimit për këtë fenomen, njohja e shenjave paralajmëruese dhe përdorimi i praktikave të sigurta në hapësirën digjitale janë hapa të rëndësishëm për parandalimin dhe adresimin e dhunës digjitale. Po ashtu, bashkëpunimi ndërmjet institucioneve publike, organizatave të shoqërisë civile dhe profesionistëve që punojnë me viktimat është thelbësor për ofrimin e mbështetjes së nevojshme dhe për forcimin e mekanizmave të mbrojtjes.

Hapësira digjitale duhet të jetë një mjedis i sigurt për të gjithë. Duke promovuar respektin për privatësinë, sigurinë dhe të drejtat e individëve, mund të kontribuojmë në krijimin e një shoqërie ku teknologjia përdoret për të fuqizuar njerëzit dhe jo për të ushtruar kontroll apo dhunë.

Siguria digjitale është pjesë e sigurisë personale. Teknologjia duhet të fuqizojë, jo të kontrollojë.