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

Rrjeti i Fuqizimit të Gruas në Shqipëri
AWEN

Lundrimi i sigurt në hapësirat digjitale

Një Toolkit për të rinjtë mbi ndërgjegjësimin, parandalimin, dhe reagimin ndaj dhunës online

Ky modul është zhvilluar në kuadër të projektit “Fuqizimi i të rinjve për të qenë të sigurt online përmes rritjes së kapaciteteve në botën digjitale”, zbatuar nga AWEN (Rjeti i Fuqizimit të Gruas në Shipëri) dhe mbështetur nga WAVE (Women Against Violence Europe).

Përgatiti: Orkidea Xhaferaj

Adresa: Rruga: “Vaso Pasha”, P.16/1, Shk 1/2, Tiranë

Web: www.awenetwork.org

Kontakt: info@awentwork.org

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

Rrjeti i Fuqizimit të Gruas në Shqipëri
AWEN

Përmbajtja

Hyrje

Qëllimi i toolkit-it

Ky toolkit u ofron të rinjve/të rejave njohuri dhe aftësi praktike për të lundruar në mënyrë të sigurt në hapësirat digjitale. Ai trajton realitetet e dhunës së lehtësuar nga teknologjia, përfshirë dhunën me bazë gjinore, ngacmimin, bullizmin kibernetik dhe shfrytëzimin që ndodh përmes teknologjive digjitale.

Bota digjitale ofron mundësi të jashtëzakonshme për lidhje, mësim dhe vetëshprehje. Megjithatë, këto mundësi shoqërohen me rreziqe që kërkojnë vetëdije dhe përgatitje. Kjo paketë e transformon cenueshmërinë e mundshme në forcë duke ju pajisur me informacion për të njohur kërcënimet, për t'u mbrojtur dhe për të reaguar në mënyrë efektive kur jeni viktima të dhunës dhe kur përjetoni dhune online.

Si të përdorni këtë toolkit

Nëse je i ri/e re dhe po e përdor këtë toolkit individualisht: Lexo çdo seksion me ritmin tënd. Përdor Kartelat e Referencës së Shpejtë në fund si kujtesa për veprimet kryesore.

Nëse je lehtësues/lehtësuese dhe e përdor në punëtori: Çdo seksion mund të përdoret si modul i pavarur. Kartelat e Referencës së Shpejtë mund të printohen veçmas si materiale ndihmëse.

Të kuptuarit e hapësirës digjitale

Çfarë është hapësira digjitale?

Hapësira digjitale përfshin të gjitha mjediset ku njerëzit ndërveprojnë përmes pajisjeve elektronike dhe rrjeteve. Kjo përfshin platforma të rrjeteve sociale (Instagram, TikTok, WhatsApp, Snapchat), aplikacione mesazhesh, mjedise lojërash online, email, faqe interneti dhe çdo hapësirë ku ndodh komunikimi digjital.

Ndryshe nga hapësirat fizike me kufij të qartë, hapësirat digjitale janë të rrjedhshme. Ato ekzistojnë në telefonin tuaj, laptopin tuaj dhe çdo pajisje të lidhur në një rrjet (internet ose përmes bluetooth). Ato janë prezente kudo, pavarësisht vendit apo zonës kohore ku ndodheni. Një bisedë që fillon në mjedis fizik mund të vazhdojë online pafundësisht.

Nëse ju krijoni përmbajtje digjitale, komente, fotografi, mundësia që ato të mbeten përjetësisht në format digjital është shumë e lartë. Sado ta fshini një mesazh apo foto, nëpërmjet kapjeve të

ekranit (screenshots), kopjeve rezervë (backup), apo arkivave online, përmbajtja e krijuar prej jush mund të jetë e përjetshme.

Andaj, kur krijoni përmbajtje digjitale, mendoni se ajo do të jetë e përjetshme.

Dhuna digjitale dhe dhuna online: A ka ndryshim?

Këto terma shpesh përdoren njëlloj, por kuptimi i dallimit mes tyre ndihmon të kuptojmë nuancat e dhunës dhe dëmit që përjetojnë viktimat e kësaj dhune.

Dhuna online i referohet akteve të dëmshme që ndodhin përmes platformave të lidhura me internetin — ngacmimeve në rrjetet sociale, bullizmit kibernetik në komente, ose kërcënimeve të dërguara në aplikacione mesazhesh.

Dhuna digjitale është term më i gjerë dhe përfshin çdo dhunë të mundësuar nga teknologjia digjitale, qoftë edhe pa internet. Këtu hyjnë:

- ngacmimi përmes SMS-ve,
- shpërndarja pa pëlqim e fotove të ruajtura në pajisje,
- përdorimi i teknologjisë për monitorimin dhe kontrollin e dikujt.

Dhuna me bazë gjinore e lehtësuar nga teknologjia i referohet dhunës digjitale që synon individët për shkak të gjinisë. Vajzat dhe gratë e përjetojnë në mënyrë disproporcionale,

përfshirë abuzimin me imazhe, ngacmimin seksual online dhe ndjekjen digjitale. Por secila gjini mund të jetë viktimë ose dhunues/e.

Pika kyçe: Dhuna në hapësirat digjitale është dhunë reale. Ajo ndikon seriozisht në shëndetin mendor, sigurinë, marrëdhëniet dhe jetën e përditshme.

Çfarë është qytetaria digjitale?

Qytetaria digjitale i referohet përdorimit të përgjegjshëm, etik dhe të sigurt të teknologjisë. Një qytetar/e digjital/e kupton të drejtat dhe përgjegjësitë e tij/saj në hapësirat online.

Të drejtat tuaja si qytetar/e digjital/e përfshijnë:

- **Privatësinë dhe kontrollin mbi informacionin tuaj personal.** Ju keni të drejtë të vendosni cilat të dhëna personale ndani, me kë dhe për çfarë qëllimi. Platformat dhe shërbimet duhet të respektojnë zgjedhjet tuaja mbi mbledhjen e të dhënave, dhe ju duhet të keni mundësinë të aksesoni, korrigjoni ose fshini informacionin që mbahet për ju.
- **Lirinë e shprehjes brenda kufijve ligjorë.** Ju keni të drejtë të shprehni mendimet tuaja, të ndani perspektivat dhe të merrni pjesë në diskutime online. Kjo e drejtë shtrihet te shprehja politike, krijuese dhe komentet shoqërore, ndonëse nuk mbron gjuhën që nxit dhunë, përbën ngacmim ose cenon të drejtat e të tjerëve.
- **Akses në informacion të saktë.** Ju keni të drejtë të kërkoni dhe të merrni informacion të vërtetë online. Kjo përfshin akses në burime arsimore, lajme, informacion shëndetësor dhe përmbajtje që ju mundëson marrje vendimesh të informuara për jetën tuaj.
- **Siguri nga ngacmimi, shfrytëzimi dhe abuzimi.** Ju keni të drejtë të përdorni hapësirat digjitale pa u ekspozuar ndaj kërcënimeve, bullizmit, ngacmimit seksual ose formave të tjera të dëmit. Askush nuk ka të drejtë t'ju bëjë të ndiheni të pasigurt online.
- **Aftësinë për të raportuar përmbajtje dhe sjellje të dëmshme.** Ju keni të drejtë të sinjalizoni shkeljet, të raportoni abuzimin dhe të merrni përgjigje nga platformat kur ndodh dëmi.

Përgjegjësitë tuaja si qytetar/e digjital/e përfshijnë:

- **Respektimin e privatësisë dhe dinjitetit të të tjerëve online.** Kjo do të thotë të mos ndani informacion personal, imazhe ose komunikime private pa pëlqimin e tyre.
- **Të menduarit kritik mbi informacionin para shpërndarjes.** Keqinformimi përhapet shpejt online. Ndarja e përmbajtjeve të pavërteta, qoftë edhe pa dashje, mund të shkaktojë dëm real. Verifikoni informacionin nga burime të besueshme para se ta shpërndani.
- **Përdorimin e teknologjisë në mënyra që nuk dëmtojnë të tjerët.** Veprimet tuaja online kanë efekte reale mbi njerëz realë. Shmangini ngacmimin, bullizmin, gjuhën e urrejtjes dhe çdo sjelljeje që mund të shkaktojë shqetësim, dëmtojë reputacionin ose rrezikojë sigurinë e të tjerëve.
- **Kuptimin e qëndrueshmërisë së veprimeve digjitale.** Përmbajtja e postuar online mund të fotografohet (screenshot), ruhet dhe shpërndahet pafund edhe pas fshirjes.
- **Mbështetjen e të tjerëve që përjetojnë dëm online.** Kur dëshmoni dhunë digjitale, keni përgjegjësinë të ofroni mbështetje dhe të mos mbeteni spektator/e pasiv/e. Kjo mund të përfshijë dëgjim pa gjykim, ndihmë për dokumentimin e abuzimit, inkurajim për raportim dhe refuzim për të marrë pjesë ose për të amplifikuar përmbajtje të dëmshme.

Çfarë është siguria në hapësirat digjitale?

Siguria në hapësirat digjitale do të thotë të kesh kontroll mbi përvojat dhe ndërveprimet e tua online. Të njohësh teknologjitë, sistemet që përdor dhe dobësitë e tyre.

Siguria gjithashtu përfshinë njohuritë dhe praktikat që ndërmerr për t'i përdorur mjetet teknologjike dhe platformat duke aplikuar cilësimet e nevojshme të sigurisë, për të mbrojtur të dhënat e tua personale.

Siguria digjitale nuk ka të bëjë me shmangien e teknologjisë. Ka të bëjë me përdorimin e teknologjisë me vetëdije, kufij dhe njohuri për të mbrojtur veten dhe për t'iu përgjigjur kërcënimeve.

Format e dhunës në hapësirën digjitale

Të kuptuarit e llojeve të dhunës digjitale ju ndihmon t'i njihni ato herët dhe të reagoni siç duhet.

Bullizmi kibernetik (Cyberbullying)

Sjellje e përsëritur e dëmshme e drejtuar ndaj një individi përmes mjeteve digjitale. Ndryshe nga bullizmi tradicional, bullizmi kibernetik mund të ndodhë në çdo kohë, të arrijë një audiencë të madhe menjëherë dhe të ndihet i pashmangshëm sepse ndjek viktimat përtej platformave dhe brenda shtëpive të tyre.

Shembuj përfshijnë: dërgim mesazhesh kërcënuese ose fyese, përhapje thashethemesh online, krijim profilesh të rreme për të tallur dikë, përjashtim i qëllimshëm i dikujt nga grupet online, postim përmbajtjesh turpëruese për dikë.

Përndjekja kibernetike (Cyberstalking)

Monitorim i vazhdueshëm, ngacmim ose sjellje kërcënuese të kryera përmes mjeteve digjitale. Kjo mund të përfshijë ndjekjen e vendndodhjes së dikujt, monitorimin e aktivitetit të tyre online, krijimin e llogarive të rreme për t'i vëzhguar, ose kontakt të padëshiruar të përsëritur.

Abuzimi i bazuar në imazhe (Image-Based Abuse)

Përfshin të gjitha aktivitetet e dëmshme që lidhen me krijimin, marrjen, përftimin, ndarjen, shpërndarjen, kërcënimin për shpërndarje, ose dërgimin pa pëlqim të imazheve ose videove intime, seksuale, ose të seksualizuara.

Format e abuzimit me imazhe:

Shpërndarja pa pëlqim e imazheve intime (Non-consensual intimate image sharing) Ndarja e imazheve intime të dikujt pa pëlqimin e tyre, përfshirë:

- ndarja e imazheve të dhëna fillimisht me besim
- postimi në media sociale ose faqe pornografike
- përcjellja te miqtë, familja ose të panjohur

Shantazhi seksual (Sextortion) Përdorimi i kërcënimeve për ndarjen e imazheve intime për të shantazhuar ose ushtruar presion mbi dikë që të prodhojë më shumë përmbajtje seksuale ose të përfshihet në veprime të tjera,për shembull, kërkesa për para ose kërcënime për të ndarë imazhet me familjen.

Regjistrimi pa pëlqim / Voyeurizmi Regjistrimi i imazheve intime të një personi të paditur, shpesh në ambiente publike ose private ku ka një pritje të privatësisë. Kjo përfshin:

- Upskirting — marrja e imazheve nën veshjet e dikujt
- Downblousing — marrja e imazheve poshtë bluzës së dikujt
- Regjistrimi i fshehtë gjatë momenteve intime

Deepfakes dhe imazhe të manipuluara digjitalisht Pornografia e falsifikuar e gjeneruar nga inteligjenca artificiale (IA) paraqet njerëz që nuk janë filmuar ose fotografuar për pornografi, por paraqiten si të tillë. Kjo përfshin ndërrimin e fytyrave në përmbajtje pornografike, aplikacione "zhveshjeje" që heqin digjitalisht veshjet nga fotot, apo çdo manipulim imazhi apo videoje për të seksualizuar imazhin e dikujt.

Cyberflashing (Imazhe seksuale të pakërkuara) Transmetimi i qëllimshëm elektronik i përmbajtjes seksualisht eksplicite të pakërkuar pa pëlqimin e marrësit. Kualifikohet si ngacmim seksual. Ndodh përmes aplikacioneve të takimeve, mesazheve direkte në media sociale, AirDrop/Bluetooth në hapësira publike.

Sexting i detyruar (Coerced sexting) Ushtrimi i presionit, detyrimi ose kërcënimi i dikujt për të krijuar dhe ndarë imazhet e tyre intime.

Ngacmimi seksual online (Online sexual harassment)

Komente, kërkesa ose përmbajtje seksuale të padëshiruar të drejtuara ndaj dikujt online. Kjo përfshin mesazhe ose imazhe seksuale të padëshiruara, komente seksuale në foto ose postime, presion për të ndarë përmbajtje intime.

Dissing / Dhuna verbale online

Kjo përfshin tallje për trupin (body shaming), komente të këqija për pamjen, fyerje të bazuara në identitet dhe poshtërim publik përmes postimeve ose komenteve.

Doxxing

Publikimi i informacionit personal të dikujt online pa pëlqim — si adresa e shtëpisë, numri i telefonit, vendi i punës ose shkolla — shpesh për të mundësuar ngacmim ose kërcënime.

Duke bërë publike këto informacione personale, viktima bëhet lehtësisht e cenueshme në botën fizike.

Vjedhja e identitetit (Identity theft)

Përdorimi i informacionit personal, imazheve ose identitetit të dikujt pa leje. Në hapësirat digjitale, kjo shpesh përfshin krijimin e profileve të rreme duke përdorur fotot dhe informacionet e dikujt.

Ekspozimi ndaj përmbajtjeve të dëmshme

Ndeshja me materiale të dhunshme, seksuale ose shqetësuese online. Kjo mund të jetë synim i qëllimshëm ose ekspozim algoritmik përmes platformave që prioritizojnë angazhimin mbi sigurinë.

Ngacmimi i koordinuar (Coordinated harassment)

Sulme të organizuara në grup që përfshijnë raportim masiv, mbytje me mesazhe urrejtjeje, fushata me hashtag, përhapje dezinformacioni.

Gjuha e urrejtjes dhe kërcënimet me bazë gjinore (Hate speech)

Përdorimi i teknologjive digjitale për të shprehur urrejtje, diskriminim dhe dhunë kundër individëve bazuar në gjini, orientim seksual, racë, etni, fe etj.

Personifikimi (Impersonation)

Krijimi i profileve të rreme, postimi i përmbajtjes shpifëse, krijimi i profileve pornografike me informacionin e viktimës, kontaktimi i punëdhënësve/familjes dhe manipulimi i rezultateve të kërkimit.

Monitorimi digjital (Digital surveillance)

Instalimi i programeve të përndjekjes pa dijeninë e viktimës, shfrytëzimi i pajisjeve "smart home" për kontroll, gjurmimi përmes llogarive të përbashkëta — veçanërisht i zakonshëm në dhunën nga partneri/ja intim/e.

Ndjellja / Grooming

Procesi i qëllimshëm i ndërtimit të besimit që synon të miturit për abuzim seksual, shfrytëzim ose trafikim përmes normalizimit gradual të sjelljes së papërshtatshme dhe krijimit të varësisë emocionale.

Kërcënimet e sigurisë kibernetike që mundësojnë dhunën digjitale

Kërcënimet e sigurisë kibernetike shpesh përdoren si mjete për të kryer dhunë digjitale. Një abuzues/e mund të përdorë teknika të hakimit (hacking), programeve keqdashëse (malware),

ose manipulimit psikologjik për të fituar kontroll mbi viktimën, për të vjedhur informacione intime, ose për të monitoruar aktivitetin e saj pa dijeni.

Phishing dhe mashtrimet në internet

Phishing është një formë mashtrimi ku kriminelët përpiqen të vjedhin informacione të ndjeshme (fjalëkalime, të dhëna bankare, informacione personale) duke u paraqitur si burime të besueshme.

Si funksionon:

- **Email phishing:** Mesazhe që duken sikur vijnë nga banka, rrjetet sociale ose institucione zyrtare
- **Smishing (SMS phishing):** Mesazhe tekst që pretendojnë të jenë nga shërbime të njohura
- **Spear phishing:** Sulme të personalizuara që përdorin informacione specifike për viktimën

Shenjat paralajmëruese:

- Mesazhe me gabime drejtshkrimore ose gramatikore
- Kërkesa urgjente për veprim të menjëhershëm
- Lidhje (links) që nuk përputhen me faqen zyrtare
- Oferta që duken "shumë të mira për të qenë të vërteta"

Malware dhe Spyware

Malware (shkurtim për "malicious software" — softuer keqdashës) përfshin çdo program të krijuar për të dëmtuar, ndërhyrë ose fituar akses të paautorizuar në pajisje dhe sisteme.

Llojet kryesore:

- **Virus:** Programi që bashkëngjitet në skedarë të tjerë
- **Trojan:** Softuer që duket i ligjshëm por përmban funksione të fshehura keqdashëse
- **Ransomware:** Program që bllokon aksesin në të dhënat tuaja dhe kërkon pagesë
- **Spyware:** Softuer që monitoron aktivitetin tuaj pa dijeni dhe dërgon informacione tek sulmuesi
- **Keylogger:** Program që regjistron çdo tast që shtypni duke kapur fjalwkapimet dhe mesazhet
- **Stalkerware:** Lloj i veçantë i spyware-it i krijuar për të monitoruar partnerët/et intimë

Stalkerware

Mund të lexojë të gjitha mesazhet, aksesojë fotot, gjurmojë vendndodhjen në kohë reale, aktivizojë kamerën dhe mikrofonin pa dijeninë e përdoruesit/es.

Shenjat që pajisja juaj mund të jetë e infektuar:

- Bateria shkarkohet shumë shpejt
- Pajisja nxehet pa arsye
- Përdorimi i të dhënave celulare është rritur papritmas
- Aplikacione të panjohura shfaqen në telefon
- Partneri/ja juaj di gjëra që nuk i keni thënë

Inxhinieria sociale (Social engineering)

Inxhinieria sociale është arti i manipulimit psikologjik që synon të bindë njerëzit të zbulojnë informacione konfidenciale. Shfrytëzon emocionet dhe prirjet natyrore njerëzore:

- Urgjenca: "Kjo ofertë skadon për 10 minuta"
- Besimi: "Unë jam nga departamenti i IT-së"
- Kurioziteti: "Shiko çfarë kam gjetur për ty"

- Dëshira për të ndihmuar: "Kam nevojë për ndihmën tënde urgjentisht"
- Lakmi: "Keni fituar një çmim të madh"

Teknikat e zakonshme:

- Pretexting: Krijimi i një skenari të rremë për të fituar besimin *"Jam kushëriri i shoqes tënde, më dha numrin tënd"*
- Baiting: Ofrimi i diçkaje tërheqëse për të joshur viktimën *USB i "humbur" me malëare, oferta shumë të mira*
- Quid pro quo: Ofrimi i një shërbimi në këmbim të informacionit *"Do t'ju ndihmoj me problemin teknik, më jepni fjalëkalimin"*
- Tailgating: Ndjekja fizike e dikujt për të fituar akses *Hyrja në ndërtesë duke u paraqitur si punonjës*
- Love bombing Vërshimi me dashuri dhe vëmendje për të manipuluar *Shpesh hapi i parë në marrëdhënie abuzive*

Shembull i një sulmi të kombinuar:

Një person merr një mesazh në Instagram nga dikush që pretendon të jetë një fotograf profesionist. Ai ofron një seancë fotografike falas. Gjatë komunikimit, ai kërkon informacione personale dhe eventualisht foto intime "për portfol." Më vonë, këto foto përdoren për sextortion.

Nga digjitalja tek fizikja – Si përshkallëzohet dhuna

Dhuna digjitale nuk mbetet e kufizuar te ekranet. Ajo rrjedh nga hapësirat digjitale në hapësira fizike. Kuptimi i modeleve të përshkallëzimit ndihmon në identifikimin e rrezikut dhe ndërhyrjen herët.

Vazhdimësia e dhunës

Dhuna shpesh ndjek një progresion:

Faza 1 — Testimi i kufijve: Kontakti fillestar që duket i pafajshëm por teston cenueshmërinë. Komplimente të tepërta, pyetje personale ose kërkesa të vogla që rriten gradualisht.

Faza 2 — Izolimi: Përpjekje për të ndarë shënjestrën nga rrjetet mbështetëse. Inkurajimi i sekretit, krijimi i konfliktit me miqtë ose familjen.

Faza 3 — Ngacmimi digjital: Sjellje e drejtpërdrejtë e dëmshme online: fyerje, kërcënime, monitorim, sjellje kontrolluese.

Faza 4 — Përshkallëzimi në hapësirën fizike: Përdorimi i informacionit të mbledhur online për të mundësuar dëm jashtë linje (offline), shfaqje në vendndodhje, kërcënime fizike, sulm.

Nga përvojat e ndara me të rinjtë/të rejat, dihet se autorët/et e zakonshëm/a të këtyre sjelljeve janë shpesh partnerët/et e rinj/reja kur ndahen. Ata/ato përdorin dhunë online si shantazh dhe shpërndarje imazhesh pa pëlqim (revenge porn) për t'u hakmarrë.

Shenjat paralajmëruese të përshkallëzimit

Vëzhgoni këto modele:

- Rritje në intensitetin ose frekuencën e kontaktit negativ
- Kërcënime që përmendin vendndodhje fizike ose jetën jashtë linje
- Përpjekje për të izoluar dikë nga miqtë dhe familja
- Sjellje monitoruese (kërkesa për vendndodhje, kontroll i mesazheve)
- Krijimi i llogarive të shumta pas bllokimit
- Ndërhyrje në rrjetet jashtë linje të shënjestrës

Ndikimi psikologjik

Dhuna digjitale ndikon në shëndetin mendor në mënyra të dokumentuara nga studimet shkencore.

Studimet tregojnë se efektet emocionale dhe psikologjike përfshijnë:

- **Rritje të ankthit dhe stresit:** Viktimave shpesh u zhvillohet ankth i vazhdueshëm për përdorimin e teknologjisë, frikë nga kontakti i papritur dhe hipervigjilencë ndaj aktivitetit online.
- **Krahasim social dhe ulje të vetëvlerësimit:** Komentet negative, sidomos ato që lidhen me pamjen fizike dhe trupin, ndikojnë thellësisht në perceptimin e vetes. Të rinjtë/të rejat raportojnë ndjenja të thella të pasigurisë pas përjetimit të talljes online.
- **Depresion dhe izolim:** Viktimat shpesh tërhiqen nga aktivitetet sociale, si online ashtu edhe jashtë linje, duke përkeqësuar ndjenjat e vetmisë.
- **Çrregullime të gjumit dhe përqendrimit:** Stresi i vazhdueshëm ndikon në aftësinë për t'u përqendruar në shkollë ose punë dhe shkakton pagjumësi.
- **Dezinformim dhe frikë:** Ekspozimi ndaj kërcënimeve dhe përmbajtjeve të dëmshme krijon një perceptim të shtrembëruar të sigurisë online.
- **Në raste të rënda:** Vetëdëmtim dhe mendime vetëvrasëse.

Këto ndikime janë reale dhe të vlefshme, jo reagim i tepruar ndaj përvojave "thjesht online".

Si të mbrohemi

Përgjegjësitë gjatë përdorimit të mjeteve digjitale

Siguria në hapësirat digjitale është një përgjegjësi e përbashkët, por ti ke fuqi të konsiderueshme mbi mbrojtjen tënde.

Menaxho gjurmën tënde digjitale

Çdo gjë që hidhet online duhet të konsiderohet si e përhershme. Kapjet e ekranit (screenshots), arkivat, kopjet rezervë (cache) apo fotografimi nga një pajisje tjetër ndikojnë në këtë përhershmëri.

Për të menaxhuar gjurmën tënde digjitale, merr parasysh:

- Çfarë informacioni rreth teje është i dukshëm publikisht?
- A mund të zbulojnë postimet e tua vendndodhjen, rutinën, shkollën apo vendin e punës?
- Çfarë mund të mësojë dikush për ty duke parë profilet e tua?

Përpara se të postoni, mendoni: si do të ndiheni nëse kjo përmbajtje do të shihej nga prindërit, familja, mësuesit/et apo punëdhënësi/ja juaj?

Kontrollo rrjetin tënd

- Prano kërkesa lidhjeje vetëm nga persona që i njeh jashtë internetit
- Rishiko periodikisht lidhjet e tua ekzistuese
- Ji i/e kujdesshëm/e se kush mund t'i shohë postimet dhe historitë e tua

Mbro informacionin tënd

Mos ndaj kurrë informacion të ndjeshëm online, duke përfshirë: adresën e plotë, numrin e telefonit, vendndodhjen aktuale, detaje të shkollës apo punës, rutinën e përditshme, informacione financiare apo dokumente identiteti.

Kërkesat minimale të sigurisë

Siguria e fjalëkalimit:

- Përdorni fjalëkalime të veçanta për çdo llogari online
- Të paktën 15 karaktere
- Kombinim i shkronjave të mëdha, të vogla, numrave dhe simboleve
- Përdorni aplikacione të besuara për të menaxhuar fjalëkalimet

Autentifikimi me dy faktorë / 2FA (Two-Factor Authentication): Aktivizoni 2FA në të gjitha llogaritë e rëndësishme si email, rrjete sociale, cloud.

Parametrat e privatësisë:

- Vendosni profilin në privat kur është e mundur
- Kontrolloni kush mund të shohë postimet dhe informacionin personal
- Çaktivizoni ndarjen e vendndodhjes
- Çaktivizoni funksionet që tregojnë kur jeni online

Mbrojtja specifike sipas platformës:

WhatsApp: Aktivizoni verifikimin me dy faktorë. Rregulloni privatësinë për foton e profilit, statusin dhe "last seen".

Instagram: Vendosni llogarinë në privat. Kontrolloni kush mund të komentojë. Përdorni funksionin Restrict.

TikTok: Aktivizoni privatësinë. Kontrolloni kush mund të komentojë, të bëjë duet apo stitch.

Snapchat: Mos harroni që kapjet e ekranit (screenshots) mund të merren. Merrni parasysh çaktivizimin e Snap Map.

Discord: Vendosni rolet dhe lejet e menaxhimit të serverit tuaj. Aktivizoni 2FA. Vendosni filtrin e mesazheve eksplicite.

Ndarja e informacionit në rrjetet sociale

Mos publikoni dokumente që përmbajnë informacione personale (psh. Nëse ke një ID apo pasaportë të re, mos e hidh online, ose nëse e hedh, fshi të gjitha informacionet e tua personale). Mos publikoni foto ndërkohë që jeni në udhëtim, vetëm pasi të jeni kthyer. Vendet që i vizitoni shpesh (psh kafja e preferuar) mos i identifikoni në përmbajtjen që ndani në rrjetet sociale.

Për prindërit e rinj

MOS POSTONI PËRMBAJTJE QË LIDHET ME FËMIJËN TUAJ. Pornografia e të miturve ka pësuar rritje në të gjithë botën. Imazhet e fëmijëve tuaj mund të përdoren në hapësira pornografike. Nëse zbulon shkollen, kopshtin, apo vende të tjera që fëmija juaj viziton, lehtësoni aksesin e dhunuesëve.

Ndarja e imazheve intime

Ndarja e imazheve intime nuk është e këshillueshme. Abuzimi i bazuar në imazhe është një nga format më të përhapura të dhunës me bazë gjinore të lehtësuar nga teknologjia.

Megjithatë, nëse dëshironi të ndani imazhe intime, mbrohuni duke:

- Mbuluar apo fshirë fytyrën tuaj, nishane identifikuese, tatuazhe apo ambiente lehtësisht të asociueshme me ju
- Kuptuar që dhënia e pëlqimit ndodh në dy faza: (1) kur imazhi krijohet dhe (2) kur imazhi ndahet me palë të tjera
- Folur me partnerin/en tuaj për ruajtjen dhe fshirjen e imazheve

Nëse nuk ndiheni komod, mos shpërndani imazhe apo video intime.

Jam dhunuar – Çfarë të bëj dhe ku të shkoj?

Nëse përjeton dhunë digjitale, nuk je vetëm dhe ekziston mbështetje.

Hapat e menjëhershëm

1. **Dokumento gjithçka:**
    - Bëj kapjen e ekranit (screenshot) të gjithë ngacmimeve, kërcënimeve apo përmbajtjes së dhunshme duke përfshirë emrat e përdoruesëve, vulat kohore, URL
    - Kap të gjithë bisedën, jo vetëm mesazhe individuale
    - Ruaj dokumentet origjinalë kur është e mundur
    - Mbaj provat, edhe pse për momentin mund të jesh e/i pavendosur nëse do ta raportosh
2. **Siguro të gjitha llogaritë** duke ndryshuar fjalëkalimet, shtuar masa sigurie dhe mbyllur sesionet aktive në pajisje të tjera.
3. **Blloko dhunuesit/et** në të gjitha platformat online, si dhe këdo që ke dijeni se mund të jetë i/e lidhur me ta.
4. **Njofto** personat e afërt menjëherë. Kërkoju ndihmë të monitorojnë platformat online.
5. **Vlerëso nëse është cënuar siguria fizike:** nëse akti përfshin doxxing apo kërcënime fizike, ndrysho rrugën e përditshme, shoqërohu nga njerëz të besuar.
6. **Mundohu të ruash jetën normale** sa më sigurt që të mundesh dhe angazhohu në aktivitete jashtë linje që të sjellin kënaqësi.

Rrugët e raportimit

Kuadri ligjor

Në Shqipëri, dhuna me bazë gjinore e lehtësuar nga teknologjia trajtohet në mënyrë të fragmentizuar. Ligji për mbrojtjen e të dhënave personale sjell parashikime në për mbrojtjen e të dhënave personale të qytetarëve. Ligji për krimet kibernetike parashikon disa vepra penale të lidhura me kompjuterin.

Raportimi në platformë

Të gjitha platformat kryesore kanë mekanizma për të raportuar ngacmime, kërcënime, imazhe të paautorizuara dhe shkelje të tjera. Dokumentoni raportimet tuaja dhe çdo përgjigje të marrë.

Shkolla ose institucioni

Nëse autori/ja i/e dhunës është një bashkëmoshatar/e nga shkolla apo universiteti yt, raporto te këshilltarët/et, psikologët/et ose administrata. Shkollat kanë përgjegjësi për të adresuar ngacmimet që ndikojnë studentët/et.

Policia e Shtetit

- Krimin kibernetik mund ta raportoni online: https://asp.gov.al/denonco-krimin-kompjuterik/
- Drejtohuni pranë Drejtorive Vendore të Policisë për raportimin e rasteve të dhunës me bazë gjinore të lehtësuar nga teknologjia

Prokuroria

Drejtohuni pranë Prokurorisë së Qarkut ku banoni: https://www.pp.gov.al/Prokurorite_prane_Gjykates_se_Shkalles_se_Pare_te_Juridiksionit_te_Pergjithshem/

Institucionet dhe organizatat mbështetëse

- **Linja Kombëtare për Gratë dhe Vajzat:** Telefononi **116 117** (24 orë, pa pagesë)
- **Alo 116 111** — Telefoni i Ndihmës për Fëmijë
- **AKSK:** https://aksk.gov.al/raporto-2/
- **iSigurt.al:** https://isigurt.al/raporto/
- **AMA:** https://ama.gov.al/ova_sev/formulare-ankese-x/
- **Hotline Albania:** https://hotlinealbania.org/siguria/
- **StopNCII.org** https://stopncii.org/?lang=sq-al

Për një listë më të plotë të organizatave mbështetëse dhe burimeve, vizitoni:
www.awenetwork.org

Pas dhunës: Hapat drejt rimëkëmbjes

Rimëkëmbja nga dhuna digjitale kërkon kohë. Dëmi është real dhe shërimi kërkon mbështetje, durim dhe burime të përshtatshme.

Pranimi i ndikimit

Nëse ke përjetuar dhunë digjitale, prano se ndjenjat e tua janë të vlefshme. Reagime të zakonshme përfshijnë:

- Ankth për përdorimin e teknologjisë ose të qenit online
- Vështirësi për të besuar të tjerët
- Turp ose siklet (edhe pse përgjegjësia i përket autorit/es të dhunës, jo ty)
- Zemërim, trishtim ose ndryshime humori
- Tërheqje nga aktivitetet sociale
- Vështirësi në përqendrim ose gjumë

Efektet kryesore të dhunës me bazë gjinore të lehtësuar nga teknologjia:

- **Psikologjike/Emocionale:** shkaktim i ankthit, depresionit, sulmeve të panikut, hipervigjilencë, rrezik i rritur për vetëlëndim
- **Shëndeti fizik:** stresi shkakton pagjumësi, probleme kardiovaskulare, dobësim të imunitetit, ndryshime në peshë
- **Fragmentizimi i sistemeve të mbështetjes:** Viktimat tërhiqen nga përditshmëria e tyre, shkëpusin lidhjet me komunitetet e tyre online
- **Ekonomike/profesionale:** Dëmtohet karriera, humbje vendi pune; kostot përfshijnë trajtim mjekësor, tarifa ligjore, masa sigurie
- **Arsimore:** Rënie e performancës akademike, rritje e braktisjes së shkollës
- **Në shoqërinë e gjerë:** Gratë dhe grupet e margjinalizuara vetë-censurohen ose qëndrojnë larg hapësirave online, duke ndikuar në uljen e zërave të ndryshëm në diskursin publik

Mbështetja psikologjike

Mbështetja profesionale mund të ndihmojë në përpunimin e përvojës dhe zhvillimin e strategjive përballuese. Merrni parasysh të flisni me:

- Një këshilltar/e ose psikolog/e shkolle
- Një profesionist/e të shëndetit mendor
- Shërbime të organizatave të specializuara në dhunën me bazë gjinore

Për burime dhe mbështetje, telefononi Linjën Kombëtare 116 117 ose vizitoni www.awenetwork.org

Metodat bazë si të përballojmë situatat e pasdhunës

Kufizo ekspozimin: Bëj pushime nga platformat ku ndodhi dëmi. Mund të tërhiqesh përkohësisht pa dhënë shpjegime.

Mbaji lidhjet: Qëndro i/e lidhur me miqtë dhe familjen mbështetëse. Izolimi mund të përkeqësojë ndikimin.

Mirëqenia fizike: Gjumi, ushqimi dhe aktiviteti fizik ndikojnë në shëndetin mendor.

Kufijtë: Je i/e lejuar të vendosësh kufij për diskutimin e asaj që ka ndodhur. Ti vendos kush di dhe sa.

Perspektiva: Veprimet e autorit/es të dhunës reflektojnë karakterin e tyre, jo vlerën tënde. Të jesh shënjestër nuk është faji yt.

Mbështetja e të tjerëve

Nëse një mik/mikeshë përjeton dhunë digjitale:

Bëj:

- Dëgjo pa gjykim
- Beso përvojën e tyre
- Mos i/e fajëso për atë që ka ndodhur
- Ndihmo t'i dokumentojnë provat, nëse dëshirojnë
- Inkurajo t'i drejtohen mbështetjes profesionale

- Respekto zgjedhjet e tyre se si të reagojnë
- Bëj kontroll periodik për t'u siguruar që janë mirë

Mos bëj:

Është shumë e rëndësishme që të mos angazhoheni në sjelljet e mëposhtme ndaj mikut/mikes tuaj viktimë:

- **Mos u përball me autorin/en e dhunës në emër të tyre pa lejen e tyre** — kjo mund të përshkallëzojë situatën dhe të vërë viktimën në rrezik më të madh
- **Mos e ndaj përvojën e tyre me të tjerë pa pëlqimin e tyre** — është e drejta e tyre të vendosin kush di dhe çfarë di

Kartelat e Referencës së Shpejtë

Kartela 1: Mbro Veten

- Përdor fjalëkalime të forta dhe unike
- Aktivizo autentifikimin me dy faktorë (2FA)
- Vendos profilin në privat
- Prano vetëm njerëz që i njeh
- Mos ndaj informacion personal publikisht
- Mendo para se të postosh — gjurmët digjitale janë të përhershme
- Ji skeptik/e ndaj mesazheve që kërkojnë informacion
- Mbaji programet të përditësuara

Kartela 2: Shenjat Paralajmëruese të Dhunës Digjitale

- Kontakt i përsëritur i padëshiruar
- Kërcënime ose frikësim përmes mesazheve/postimeve
- Sjellje monitoruese — kërkon të dijë vendndodhjen ose aktivitetet
- Shpërndarje e informacionit ose imazheve pa pëlqim

- Tentativa për të të izoluar nga miqtë/familja
- Krijim i llogarive të reja pas bllokimit
- Mesazhe që të bëjnë të ndihesh keq, i/e frikësuar apo i/e kontrolluar

Kartela 3: Nëse Përjeton Dhunë

1. MOS U ANGAZHO me autorin/en
2. DOKUMENTO gjithçka (kapje ekrani me data)
3. BLLOKO dhe RAPORTO në platformë
4. SIGURO llogaritë (ndrysho fjalëkalimet, aktivizo 2FA)
5. NJOFTO një person të besuar
6. RAPORTO tek autoritetet nëse ka kërcënime serioze
7. KËRKO MBËSHTETJE për shëndetin mendor

Linja Kombëtare: 116 117

Kartela 4: Mbështetja e një Miku/Mikeshe

Bëj:

- Dëgjo pa gjykim
- Beso përvojën e tyre
- Mos i/e fajëso
- Ndihmo me dokumentimin nëse dëshirojnë
- Inkurajo mbështetjen profesionale
- Respekto zgjedhjet e tyre
- Kontrollo përsëri pas një kohe

Mos bëj:

- Mos kontakto autorin/en e dhunës pa lejen e mikut/mikes — kjo mund t'i vërë ata/ato në rrezik më të madh
- Mos ndaj përvojën e tyre me të tjerë pa pëlqimin e tyre

Referenca

Mertiri, E. (2024). *Manuali i Trajnimit të Sigurisë Kibernetike: Mbrojtja e hapësirave dixhitale për gratë, studentët dhe prindërit.* AWEN Network.

UNFPA (2021). *Technology-facilitated Gender-based Violence: Making All Spaces Safe.* https://www.unfpa.org/TFGBV

UN Women (2023). *Expert Group Meeting Report: Technology-facilitated Violence against Women: Towards a Common Definition.* https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technology-facilitated-violence-against-women

UN Women (2024). *Technology-facilitated gender-based violence: Developing a shared research agenda.* https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda

UN Women. *FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls.* https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

UNDP (2024). *Analysis of Technology-Facilitated Gender-Based Violence.* https://www.undp.org/sites/g/files/zskgke326/files/2024-12/undp-executive-summary-en.pdf

McGlynn, C., & Rackley, E. *Image-Based Abuse.* University of Durham. https://www.claremcglynn.com/image-based-abuse

Powell, A. & Henry, N. (2017). *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse.* RMIT University. https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf

Hellevik, P. M., Haugen, L. E. A., & Överlien, C. (2025). *Outcomes of image-based sexual abuse among young people: a systematic review.* European Journal of Psychotraumatology. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1599087/full

End Cyber Abuse. *Image-Based Sexual Abuse – An Introduction.* https://endcyberabuse.org/law-intro/

Nixon, C. L. (2014). *Current perspectives: the impact of cyberbullying on adolescent health*. Adolescent Health, Medicine and Therapeutics, 5, 143–158. https://pmc.ncbi.nlm.nih.gov/articles/PMC4126576/

Zhu, C., et al. (2021). *Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures.* Frontiers in Public Health. https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2021.634909/full

BMC Psychiatry (2023). *Prevalence and related risks of cyberbullying and its effects on adolescent.* https://bmcpsychiatry.biomedcentral.com/articles/10.1186/s12888-023-04542-0

The Lancet Regional Health – Americas (2025). *Cyberbullying, mental health, and substance use experimentation among early adolescents: a prospective cohort study.* https://www.thelancet.com/journals/lanam/article/PIIS2667-193X(25)00012-2/fulltext

Chatterjee, R., et al. (2018). *The Spyware Used in Intimate Partner Violence.* IEEE Symposium on Security and Privacy. https://ieeexplore.ieee.org/document/8418618/

Rogers, M. M., et al. (2023). *Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review.* https://pmc.ncbi.nlm.nih.gov/articles/PMC10486147/Technology Safety (NNEDV). *Spyware / Stalkerware Overview.* https://www.techsafety.org/spyware

Thorn (2025). *Sexual Extortion & Young People: Navigating Threats in Digital Environments.* https://www.thorn.org/research/library/sexual-extortion-young-people/

Patchin, J. W., & Hinduja, S. (2020). *Sextortion Among Adolescents: Results From a National Survey of U.S. Youth*. Sexual Abuse, 32(1), 30–54. https://journals.sagepub.com/doi/abs/10.1177/1079063218800469

Ray, A., & Henry, N. (2025). *Sextortion: A Scoping Review.* Trauma, Violence, & Abuse. https://pmc.ncbi.nlm.nih.gov/articles/PMC11558931/

INHOPE. *Recognising the Stages of Grooming.* https://www.inhope.org/EN/articles/the-stages-of-grooming

NSPCC Learning. *Grooming: recognising the signs.* https://learning.nspcc.org.uk/safeguarding-child-protection/grooming

Tech Coalition. *Online Grooming: Considerations for Detection, Response, and Prevention.* https://technologycoalition.org/

Winters, G., & Jeglic, E. (2022). *Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molesters.* Deviant Behavior. https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197656

Umbach, R., Henry, N., Beard, G., & Berryessa, C. (2024). *Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries.* CHI Conference on Human Factors in Computing Systems. https://dl.acm.org/doi/fullHtml/10.1145/3613904.3642382

Learning Network, Western University. *What You Need To Know About Non-Consensual Sexual Deepfakes.* https://www.gbvlearningnetwork.ca/our-work/infographics/nonconsensualsexualdeepfakes/index.html

Policia e Shtetit – Denonco krimin kompjuterik: https://asp.gov.al/denonco-krimin-kompjuterik/

Prokuroritë pranë Gjykatës së Shkallës së Parë: https://www.pp.gov.al/Prokurorite_prane_Gjykates_se_Shkalles_se_Pare_te_Juridiksionit_te_Pergjithshem/