

UOC

Toolkit UOC: Estratègies i eines per protegir-nos davant de les violències masclistes digitals



Pacte d'Estat
contra la violència de gènere

Universitat Oberta
de Catalunya

Introducció



Onlife: la connexió entre el món digital i l'analògic

Actualment, utilitzem les tecnologies i ens connectem en línia per fer moltes coses de la nostra vida quotidiana: cercar informació, estudiar, relacionar-nos amb les amistats, lligar, fer tràmits i gestions, jugar, comprar, etc. **Podem separar la nostra vida analògica de la digital, quan estan totalment interrelacionades?** Gairebé impossible. És per això que hem de tenir en compte que tot el que vivim a l'espai digital i a través de les xarxes socials també ens afecta físicament i emocionalment, i que, per tant, té conseqüències en molts aspectes de la nostra vida: en què estudiem, en com i amb qui ens relacionem i en els espais on participem, entre d'altres.



La doble cara de les TRIC

De la mateixa manera que ens obren un ventall d'espais i d'oportunitats, **les tecnologies de la relació, la informació i la comunicació (TRIC) també es poden convertir, malauradament, en un terreny propens a l'exercici de violències masclistes, LGTBI-fòbiques i racistes**, entre d'altres.

Violències com el seguiment i la vigilància, el control, l'assetjament en línia o l'exhibicionisme sexual es fan presents de manera cada vegada més intensa als espais digitals, i prenen formes noves.



Les violències masclistes digitals a la universitat

Alguns estudis mostren que **el percentatge de violències masclistes digitals (VMD) en entorns universitaris pot oscil·lar entre un 10 % i un 35 %**, taxes que poden arribar a ser superiors a les de la població adolescent. Amb relació als espais digitals personals i institucionals, el projecte SeGReVUni, que té entre els seus objectius visibilitzar i dimensionar les violències de gènere a les universitats de Catalunya, mostra que l'alumnat percep més inseguretat en els espais virtuals personals que en els institucionals (Moodle, correu corporatiu, etc.). Per exemple, en els primers, la inseguretat representa un 20,1 %, comparat amb el 8,5 % en el cas dels segons.



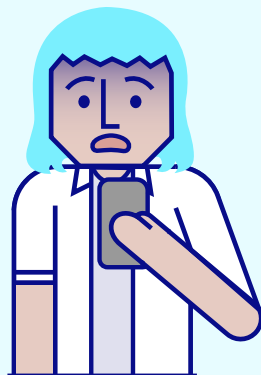
El Toolkit UOC, per protegir-te de les violències masclistes digitals

En el marc d'una universitat digital com la UOC, que ofereix una formació 100 % en línia, volem encarar el repte de promoure espais digitals més segurs i lliures de violències masclistes, i per això considerem important oferir aquest recurs. **Aquest Toolkit vol dotar-nos de coneixements per identificar més i millor les violències masclistes** que es poden donar en els espais digitals, i dotar-nos d'algunes eines i estratègies per poder-les prevenir i/o mitigar.

Quins tipus de violències masclistes ens trobem en el món digital?

Les violències masclistes digitals tenen formes diverses i ens afecten de moltes maneres.

Només si sabem identificar-les, les podrem combatre. En aquest Toolkit, i seguint la classificació de Donestech, posem el focus en àmbits de violències masclistes digitals (VMD) on aquestes es donen més sovint: l'assetjament en línia, les violències sexuals digitals i el control i vigilància digital.



01

Assetjament en línia o ciberassetjament

Són violències amb discursos altament masclistes, per raó de sexe i/o gènere i/o orientació sexual. Busquen disciplinar les dones perquè retornin als seus rols tradicionals, i també menystenir les dones i les persones LGTBIQ+, així com els seus èxits. Poden ser efectives i aconseguir que se sentin menys capaces, i que, fins i tot, abandonin els espais d'estudi, de treball i de poder que mereixien, així com les tecnologies o xarxes socials que fan servir.

02

Violències sexuals digitals

Són les accions en què s'utilitzen mitjans tecnològics per vulnerar la intimitat, la dignitat o el consentiment d'una persona amb finalitats sexuals. Busquen danyar a través de la humiliació i la vergonya pública, a més de controlar els cossos i la sexualitat de les dones i les persones LGTBIQ+.

03

Control i vigilància digital

És una de les violències més perpetrades en l'àmbit de les relacions sexoafectives, i també una de les més reconegudes. Se sustenten en el mite de l'amor romàntic i en estereotips sexistes. Solen donar-se de manera gradual i progressiva: hi trobem des d'accions menys tecnològiques, com el control dels horaris de connexió i activitat en línia, fins a accions més sofisticades, com el monitoratge dels moviments de la persona a través de comptes o dispositius de rastreig.

Com es manifesten les violències masclistes digitals?

En les tres tipologies de violències masclistes digitals **trobem diferents actituds, accions o situacions** que és essencial conèixer per poder identificar-les i protegir-nos. També tenen un paper clau en la prevenció.

01

Assetjament en línia o ciberassetjament

En l'assetjament en línia trobem:

Insults sexistes i expressions discriminatòries

Missatges emesos contra les dones o les persones no binàries amb la intenció d'insultar o denigrar, que reflecteixen patrons culturals masclistes basats en rols tradicionals, amb la qual cosa s'accentuen estereotips i prejudicis. D'aquests, malauradament, a les xarxes socials en podem trobar molts del tipus “ves a fregar plats”, “calladeta estàs millor” o “les lesbianes sou unes reprimides”, per donar-ne alguns exemples.

Discurs d'odi

És l'acció comunicativa que té com a objectiu promoure i alimentar una opinió prejudiciosa, errònia, estigmatitzadora i destructiva cap a un grup d'individus històricament discriminat o perseguit per motius racials, ètnics, religiosos, d'origen nacional, d'orientació sexual, d'identitats de gènere o de discapacitat, entre d'altres.

Amenaces

Són continguts violents, lascius o agressius que manifesten una intenció de fer mal. Les amenaces poden ser múltiples i poden comportar agressió física i/o sexual.

Desprestigi i difamació

És la desqualificació de la trajectòria, la credibilitat o la imatge pública d'una persona a través de l'exposició d'una informació falsa, manipulada o fora de context.

Censura i silenciament

Són atacs específics que provoquen la retirada de continguts o el tancament de perfils de les afectades.

Dòxing

És la publicació de dades personals d'algu, com el seu número de telèfon o l'adreça on viu, sense el seu consentiment. Poden exposar públicament aquesta persona.

Suplantació d'identitat

Ús del perfil d'algu sense el seu consentiment, o creació d'un o més perfils falsos amb la intenció de fer-se passar per una altra persona.



02

Violències sexuals digitals

Quins tipus de violències sexuals digitals ens podem trobar?:

Sextreading o pornodifusió no consentida

Consisteix en el registre, l'emmagatzemament i/o la publicació de contingut de caràcter íntim o sexual (fotos, missatges i/o vídeos) sense el consentiment de la persona. Les imatges es poden obtenir de la pràctica del sexting o bé a través de múltiples estratègies o pràctiques, com el robatori, l'extorsió o l'enregistrament no consentit.



ATENCIÓ! No confonguem el sexting, que és l'enviament de contingut de caràcter íntim o sexual de manera consentida i lliure, amb el sextreading, que és una agressió sexual.

Sextorsió

Es dona quan l'agressor té imatges íntimes d'una persona i l'extorsiona mitjançant l'amenaça de publicar-les. Pot extorsionar demanant diners, més fotografies íntimes o relacions sexuals.

L'exhibicionisme sexual o cyberflashing

Es dona quan l'agressor envia imatges sexualment explícites o indegudes sense consentiment de la persona que les rep, sovint mitjançant WhatsApp, Bluetooth o AirDrop, o a través de les xarxes socials. És una pràctica que acostuma a crear situacions d'incomoditat, vulneració de la intimitat i assetjament.

Slut-shaming o titllar de "puta"

És el terme que descriu la pràctica d'avergonyir, criticar o culpar les persones, especialment les dones, per la seva sexualitat o pels seus comportaments sexuals. Aquesta conducta implica utilitzar llenguatge despectiu i judicis morals, com ara etiquetar algú de "puta" o de "fresca", amb l'objectiu de minar la seva reputació i autoestima.

Deepfakes sexuals o nudes

El *deepfake* sexual, *nude* o hipertrucatge és la manipulació, mitjançant IA, de contingut audiovisual (vídeos, fotografies, audios) que inclou material sexual, amb la intenció de danyar, humiliar o difamar una persona. Els primers casos han estat amb dones famoses, però l'accés gratuït a aquestes aplicacions està fent que proliferin els *deepfakes* sexuals.

03

Control i vigilància digital

Situacions de control i vigilància digital:

El control i vigilància digital en les relacions

Normalment, el control i la vigilància en el marc d'una relació no arriben de cop i volta, sinó que es donen de manera gradual i progressiva. Poden començar amb conductes més difícils d'identificar o més normalitzades, com ara:

- **Controlar els horaris de connexió i activitat en línia.**
- **Exigir de manera constant a la parella, amb la geolocalització, que digui on és en tot moment.**
- **Obligar a mostrar els missatges de xat amb una altra persona.**
- **Mostrar enuig per no tenir sempre una resposta immediata en línia.**
- **Utilitzar perfils de xarxes socials comuns per controlar què publica o qui són les amistats.**
- **Interferir en relacions que la parella té amb altres persones a internet.**
- **Censurar fotos que la parella publica i comparteix a les xarxes socials.**
- **Espiar el mòbil de la parella.**
- **Comprometre la parella a facilitar les contrasenyes.**
- **Exigir imatges i vídeos íntims.**



El control i la vigilància d'acció tecnològica

D'altra banda, hi ha altres maneres de control i vigilància digital que requereixen més acció tecnològica per poder-les exercir i que sovint es fan sense el consentiment i/o coneixement de l'altra persona:



Accés il·lícit als comptes

De les xarxes socials, Google o iCloud, el correu electrònic, les plataformes de *streaming*, les compres en línia, el WhatsApp web, etc. Aquest accés pot venir donat perquè la persona coneix o pot endevinar fàcilment les contrasenyes de la parella, o bé perquè comparteixen dispositius i hi té accés fàcilment. Tenir accés a aquests comptes proporciona molta informació sobre nosaltres: el nostre historial d'activitat i d'ubicació, fotos, fitxers, documents, gestor de contrasenyes, etc.

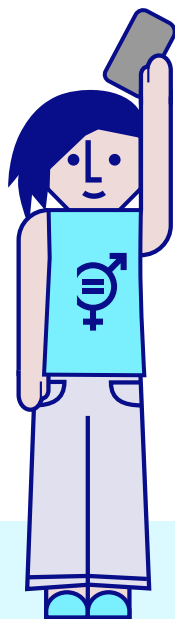


Geolocalització

La geolocalització és la capacitat per obtenir la ubicació geogràfica real d'una persona mitjançant algun dispositiu, utilitzant un sistema de GPS, Bluetooth i/o connexió a internet. Es pot donar perquè la persona té accés al compte de Google o iCloud de la parella, o bé perquè comparteixen algun dispositiu que geolocalitza, com ara uns AirPod; o també perquè pot haver col·locat un dispositiu de rastreig com l'AirTag a la bossa o al cotxe, per exemple.

Saps què és l'autodefensa feminista digital?

La manera més eficaç d'erradicar les violències masclistes és posar el focus en els agressors perquè deixin d'exercir aquestes violències. Però, mentre no aconseguim aquest món lliure de violències i equitatiu pel qual treballem, cal posar-se en marxa per aprendre a prevenir aquests actes, i perquè les dones i les persones LGTBIQ+ desenvolupem eines de protecció. Una d'aquestes eines és l'autodefensa feminista.



Què implica, l'autodefensa feminista digital?

L'autodefensa feminista en l'àmbit digital implica acompanyar l'apoderamentament personal i col·lectiu de les dones i les persones LGTBIQ+ per prendre el control de les seves dades, comptes i dispositius.

Per respondre a les VMD, cal que enfoquem la seguretat des d'una mirada holística, que inclogui la dimensió digital però també la física, la de les cures i l'emocional, ja que totes estan interrelacionades. La seguretat, doncs, és una noció profundament personal, subjectiva i travessada pel gènere.

Desigualtats davant de les violències masclistes digitals

No totes estem en igualtat de condicions per afrontar les violències digitals. Les dones i les persones LGTBIQ+, racialitzades o indígenes, i, en definitiva, les persones que pertanyen a una comunitat tradicionalment discriminada, estan més exposades a patir VMD. De la mateixa manera, aquestes persones no tenen els mateixos recursos i capacitats per prevenir-les, mitigar-les i sobrepassar-les.

Suport i eines per combatre les violències masclistes digitals

Recorda que tenir una xarxa de suport i solidaritat marca la diferència a l'hora d'afrontar les VMD. Per això, a l'última pàgina t'oferim una sèrie de recursos a través dels quals es pot demanar suport i ajuda.

A continuació, oferim una sèrie d'estratègies i eines d'autodefensa feminista digital per respondre a aquestes violències masclistes digitals i mitigar-les.

Què pots fer si pateixes assetjament en línia o violències sexuals digitals?

Documentar els atacs

Documentar els casos de VMD és fonamental per bastir una estratègia de resposta. El registre exhaustiu dels atacs serveix per conèixer la magnitud i l'abast de l'atac, i el *modus operandi* de la persona atacant, i també ens pot ajudar a avaluar si les respostes que implementem, com ara silenciar o bloquejar, mitiguen o acaben potenciant la violència.



En **aquesta fitxa**  trobaràs els passos necessaris per documentar-ne cada cas.



Recopilar i guardar l'evidència

Davant de casos d'assetjament en línia, dòxing, amenaces, *sexpredding*, etc., és recomanable preservar-ne l'evidència per si es decideix denunciar per la via judicial o per altres vies. Si no ho fem, les persones atacants podrien esborrar les proves i, aleshores, el procés no es podria dur a terme. Hem de tenir en compte que, per acreditar agressions davant d'un jutjat, les captures de pantalla no són suficients, ja que es tracta d'un material que es podria manipular fàcilment, i s'han de certificar.



En aquestes dues fitxes trobaràs els passos necessaris per recopilar i certificar evidència:

-  **Fitxa 1**
-  **Fitxa 2**



Reportar, silenciar i bloquejar

Tot i que encara no hi ha mecanismes accessibles, efectius i transparents per protegir-nos davant de les VMD, totes les plataformes disposen d'algun canal per comunicar i reportar, mitjançant formularis, vulneracions de la privacitat o la publicació de continguts inapropiats. És important fer servir aquests mecanismes de les plataformes si això ens ha de fer sentir millor. No tenim l'obligació de viure situacions que ens generin malestar o ansietat. Un cop s'ha reportat i certificat el cas, és útil i/o desitjable bloquejar els comptes d'usuari que ens estan assetjant o atacant.



En **aquesta fitxa**  trobaràs els passos necessaris per silenciar i bloquejar.

En **aquesta fitxa**  trobaràs tutorials sobre com reportar a cada plataforma.



Exigir a les plataformes que retirin el contingut

Exigir a les plataformes (xarxes socials, serveis de missatgeria, pàgines web, etc.) que retirin immediatament els continguts d'amenaça, o les imatges o vídeos íntims publicats, que tinguin allotjats sense consentiment. Es pot consultar com fer-ho [aquí](#) .

També es pot sol·licitar la retirada immediata d'una publicació de contingut íntim o sexual a través del **Canal Prioritari de l'Agència Espanyola de Protecció de Dades (AEPD)** [aquí](#) .

Mostrar rebuig cap a l'agressor

Quan presenciem una situació de violència masclista digital, és fonamental actuar per donar suport a la víctima i contribuir a aturar l'agressor. A continuació, es detallen algunes accions que podem emprendre:

Mostra el teu rebuig cap a l'agressor:

- No participis en l'agressió ni hi donis suport: evita compartir, comentar o fer "m'agrada" a continguts que humiliïn o ataquin la persona.
- Expressa la teva desaprovació: si coneixes l'agressor, comunica-li que la seva conducta és inacceptable i que ha de cessar de fer-ho immediatament.

Dona suport a la víctima:

- Ofereix ajuda: posa't en contacte amb la persona afectada, escolta-la i ofereix-li el teu suport.
- Contribueix a formar una xarxa de suport i cura per ajudar a documentar i reportar els fets quan calgui.
- Anima-la a buscar ajuda professional: recomana-li que es posi en contacte amb serveis d'atenció especialitzada com els que afegim al final del kit.

Crear una xarxa de suport i cura

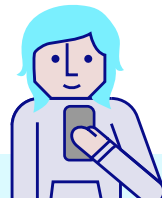
Quan vivim una amenaça o un atac, el primer que cal fer és atendre el nostre benestar emocional i personal, i establir una xarxa de suport i cura. Podem necessitar distanciar-nos de les xarxes socials, ja sigui momentàniament o durant períodes llargs. Podem passejar, llegir, dibuixar, meditar o fer coses que ens ajudin a relaxar-nos al marge dels dispositius electrònics. També caldrà que busquem amistats o familiars i els expliquem què necessitem en aquest moment, perquè ens puguin ajudar a enfrontar-nos a l'atac. Una bona idea és que aquestes persones de confiança reportin, certifiquin evidència i bloquegin contingut violent en lloc nostre fins que la situació es calmi.



En [aquesta fitxa](#)  trobaràs algunes tècniques de cura personal.



Davant del control o la vigilància digital, què pots fer?



Mapatge de comptes i dispositius compartits

- ✓ Cal identificar quins comptes i dispositius es comparteixen o s'han compartit, o estan relacionats o sincronitzats entre ells, en la relació amb aquesta persona: ordinador, tauleta, plataformes d'estríming, xarxes socials, pàgines de compra en línia, pla de telefonia familiar, etc.
- ✓ És important que hi inloguis també tots els comptes administratius i/o comptes en què arriben diners.



En aquesta [fitxa](#) et donem unes plantilles per fer el mapatge.

Tancar els comptes i canviar les contrasenyes

- ✓ Tanca els comptes en qualsevol dispositiu al qual aquesta persona tingui accés i obre comptes nous dels quals tinguis el control exclusiu.
- ✓ Revisa la configuració de seguretat i privadesa de les xarxes socials i activa, sempre que sigui possible, la verificació en dos passos. [Aquí](#) t'expliquem com fer-ho.
- ✓ Pensa si algú podria esbrinar les contrasenyes, o si pot haver tingut accés físic als teus dispositius.
- ✓ Canvia les contrasenyes dels comptes i els codis d'accés (PIN) que utilitzis per desbloquejar els dispositius (mòbils, ordinadors, tauletes). Pensa també en els dispositius connectats a la casa, com ara el rúter i els assistents de veu.



[Recordem que cal fer servir contrasenyes segures!](#)

Desconnectar

- ✓ Pregunta't si actualment estàs connectada a algun dispositiu compartit (auriculars sense cable, assistents de veu, tauletes...), i desconnecta'l si pots.



[En aquesta guia exhaustiva](#) podràs seguir-ne, pas a pas, totes les indicacions.

La cura digital, al centre

Posar la cura digital al centre significa adoptar pràctiques de protecció, tant en l'àmbit individual com en el col·lectiu, per garantir un espai digital més segur i resilient. Aquesta protecció es pot dividir en quatre àmbits clau:

L'autocura digital

Implica adoptar bones pràctiques per protegir les nostres dades i dispositius. Inclou, entre d'altres, gestionar de manera segura els comptes, actualitzar les aplicacions per evitar vulnerabilitats, utilitzar connexions segures (HTTPS), evitar xarxes wifi públiques sense protecció i ser conscients dels rastres digitals que deixem a les grans tecnològiques (*big techs*).

Cura del grup

Les pràctiques digitals segures no només ens protegeixen a nosaltres, sinó també a la nostra comunitat. Per això, és important seguir pràctiques com: utilitzar aplicacions de missatgeria amb xifratge d'extrem a extrem i evitar compartir informació sensible en canals insegurs; o no exposar informació de terceres persones sense el seu consentiment i utilitzar eines que permetin gestionar la privacitat dels nostres grups i xarxes socials.

Cura dels dispositius

Els dispositius que fem servir són portes d'entrada a la nostra informació personal. Mantenir-los segurs és fonamental, amb pràctiques com instal·lar programari de seguretat i revisar-ne la configuració de privacitat, o assegurar-nos que les aplicacions descarregades siguin segures i provenguin de fonts fiables, o bé instal·lar un antivirus fiable.

Cura de la informació

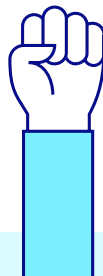
La informació és un dels actius més valuosos a l'era digital, per això cal protegir-la adequadament amb pràctiques com utilitzar eines de xifratge per protegir dades sensibles i evitar que siguin accessibles en cas de pèrdua o robatori del dispositiu, o bé eliminar contingut sensible amb aplicacions d'esborrament segur.

En aquest [enllaç](#) es despleguen eines concretes molt interessants per a cadascuna de les dimensions de la cura digital.



Fortificació dels nostres dispositius i comunicacions

De la mateixa manera que procurem que a casa nostra no entri ningú que no vulguem, en el nostre àmbit digital podem fer el mateix. **Recorda el lema: els nostres dispositius, les nostres regles!**



Aquí presentem alguns consells bàsics per fortificar-nos:



Tenir contrasenyes fortes, segures i diverses

Podem trobar més detalls sobre contrasenyes segures [aquí](#).



Apagar el GPS, la connexió wifi i el Bluetooth quan no els fem servir

En general, no és bona idea mantenir una porta oberta als nostres dispositius que permeti la connexió d'altres persones. A més de comportar un malbaratament d'energia, mantenir aquestes connexions disponibles quan no les fem servir pot facilitar intrusions il·legítimes i atacs.



Cobrir la càmera i el micròfon del dispositiu amb una cinta o adhesiu

Podem dissenyar adhesius especials per a la nostra càmera! També podem utilitzar protectors de privacitat de la pantalla. És una manera senzilla d'assegurar que ningú obté imatges nostres sense el nostre permís.



Gestionar les identitats

No hi ha una única manera de ser presents a internet i de relacionar-nos amb les xarxes socials. Les diferents opcions que tenim a l'abast a l'hora de gestionar la nostra identitat digital ens permeten decidir què volem compartir en cada moment. Tenir diferents perfils per gaudir dels nostres interessos diferents és una manera senzilla de dificultar atacs i mantenir el control sobre l'accés a la nostra informació personal. Aquesta tècnica s'anomena *compartimentació d'identitat*.



En [aquest enllaç](#) hi ha més idees sobre com gestionar les nostres identitats digitals.

Recursos



**Fembloc. Línia
feminista d'atenció
i suport a les
violències masclistes
digitals**



**Protocol per a
la prevenció, la
detecció, l'actuació
i la resolució
de situacions
d'assetjament sexual
i assetjament per raó
de sexe, d'orientació
sexual i d'identitat
i/o expressió de
gènere de la UOC**



**Normativa contra
l'assetjament sexual
i la discriminació
per raó de sexe,
d'orientació sexual
i d'identitat i/o
expressió de gènere
de la UOC**



Aquest kit ha estat elaborat per Donestech.

Barcelona
Bogotà
Ciutat de Mèxic
Madrid
Palma
Sevilla
València

Seu central
Rambla del Poblenou, 154-156
08018 Barcelona
(+34) 932 532 300

Totes les seus a
seus.uoc.edu

uoc.edu

✕ **[@UOCuniversitat](https://twitter.com/UOCuniversitat)**

✕ **[@UOCrespon](https://twitter.com/UOCrespon)**

▶ **[UOC](https://www.youtube.com/UOC)**

▶ **[UOC.universitat](https://www.facebook.com/UOC.universitat)**