ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF
Centre de documentation
sur l'éducation des adultes et la condition féminine

Boîte à outils : Cyberintimidation chez les adultes

Cette boîte à outils vise à combler le manque de documentation sur les différentes formes que peut prendre la cyberintimidation dans les communautés d'adultes, particulièrement la cyberintimidation visant les femmes. En effet, il existe de nombreuses ressources pour comprendre et prévenir l'hostilité en ligne chez les jeunes, mais il y a peu d'information sur les violences en ligne vécues par les femmes. Celles-ci font pourtant partie des personnes les plus visées par ces agressions. Cette boîte à outils est le fruit d'un travail collaboratif avec plusieurs communautés qui ont partagé leurs expériences et ont alimenté la recherche de solutions pour encourager la création d'un espace sécuritaire sur internet.

Dans la boîte à outils en ligne, vous aurez accès à du contenu téléchargeable et imprimable (une affiche, des fiches pratiques, un guide synthétique), mais aussi à de courtes capsules d'information animées.

Consultez la boîte à outils complète sur le site du CDÉACF à l'adresse suivante : https://cdeacf.ca/boite-outils-cyberintimidation

469, rue Jean Talon Ouest, bureau 229, Montréal (Québec) H3N 1R41
1 514 876-1180 | info@cdeacf.ca | CDEACF.ca

Liste des outils disponibles

Documents imprimables

Vous trouverez dans la boîte à outils en ligne 7 fiches qui présentent différents types de violences en ligne :

- Les agressions
- La diffamation
- La discrimination
- Le doxxing
- Le gaslighting
- Le harcèlement
- La sextorsion

La boîte à outils contient aussi :

- 1 fiche qui présente quelques cyberastuces qui peuvent être utiles selon le contexte
- 1 fiche qui partage certaines stratégies de résistance utilisées par les milieux
- 1 petite affiche synthèse « Créez votre nétiquette en 4 questions clés »
- 1 guide détaillé en 2 pages pour vous guider dans la formulation de votre nétiquette.

Capsules vidéo

Vous trouverez dans la boîte à outils en ligne les 3 capsules de la courte série « La cyberintimidation : des violences en ligne aux impacts réels »

- Capsule 1 : Un bref portrait
- Capsule 2 : Les types de violences
- Capsule 3 : Les stratégies de résistance.

ENSEMBLE CONTRE l'intimidation
Avec la participation financière de : Québec
CDEACF Centre de documentation sur l'éducation des adultes et la condition féminine

1.TYPOLOGIES

LE DOXXING

Qu'est-ce que c'est?

C'est la diffusion, sans consentement, de vos informations confidentielles, de celles de votre groupe ou de votre organisation.

Le but est de permettre de vous identifier ou de vous trouver, pour vous faire du tort.

Exemples

Révéler l'adresse d'une maison d'hébergement, c'est du doxxing.

Utiliser la géolocalisation pour révéler où vous vous trouvez, c'est du doxxing.

Faire croire qu'un criminel est caché chez vous pour que la police vienne à votre domicile, c'est du doxxing… c'est même du swatting!

Révéler votre nom pour vous identifier de force, alors que vous utilisez un pseudonyme en ligne, c'est du doxxing.

VERSO : STRATÉGIES DE RÉSISTANCE →

LE DOXXING

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Partager ses expériences ;

Protéger sa vie privée ;

S’entraider dans des groupes de soutien ;

S'anonymiser.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LA DISCRIMINATION

Qu'est-ce que c'est?

C'est cibler vos caractéristiques identitaires ou celles de votre groupe de façon négative dans le but de vous rabaisser, vous exclure ou inciter à la violence contre vous.

Les caractéristiques identitaires d'une personne ou d'un groupe sont, par exemple : son origine ethnique, son identité de genre, son orientation sexuelle, son apparence physique, son âge, ses particularités neurologiques ou ses handicaps.

La haine en ligne se diffuse par tous les moyens, notamment en images ou par écrit. Elle peut alimenter et encourager la discrimination.

Exemples

Se moquer de votre accent dans les commentaires d'une vidéo, c'est de la discrimination.

Vous insulter à cause de votre poids, c'est de la discrimination.

Écrire en commentaire que vous êtes une voleuse parce que vous êtes immigrante, c'est de la discrimination.

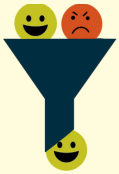
Remettre en question votre genre parce que vous êtes une gameuse qui joue bien, c'est de la discrimination.

VERSO : STRATÉGIES DE RÉSISTANCE →

LA DISCRIMINATION

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Modifier le genre perçu du profil ;



Utiliser la modération automatique ;

Créer deux profils ;

Dénoncer l'adversaire.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LA DIFFAMATION

Qu'est-ce que c'est?

Nuire à votre réputation en diffusant des informations, qu'elles soient vraies ou fausses, c'est de la diffamation.

L'objectif est de vous rabaisser, vous ridiculiser ou provoquer de la haine contre vous.

Exemples

Écrire sur un réseau social que vous avez une ITSS pour se venger de votre rupture, c'est de la diffamation.

Révéler des informations, vraies ou fausses, sur un réseau professionnel, pour nuire à votre promotion, c'est de la diffamation.

Partager une fausse rumeur sur vous sous prétexte qu'elle est drôle, c'est de la diffamation.

Usurper votre identité pour publier des contenus qui vont discréditer votre militantisme, c'est de la diffamation.

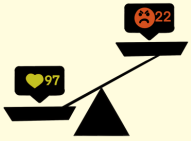
VERSO : STRATÉGIES DE RÉSISTANCE →

LA DIFFAMATION

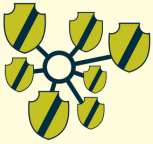
EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Protéger sa vie privée ;

Rencontrer les autorités ;



Aimer les commentaires ;



Mobiliser une communauté d'allié-e-s.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LES AGRESSIONS EN LIGNE

Qu'est-ce que c'est?

C'est la publication privée ou publique d'insultes ou de menaces, contre vous ou vos proches.

Parfois une agression cible votre identité : votre origine ethnique, votre identité de genre, votre orientation sexuelle, votre apparence physique, votre âge, vos particularités neurologiques ou votre handicap, notamment. Dans ce cas c'est une agression discriminatoire.

L'objectif est de vous rabaisser, pour vous exclure d'un groupe ou d'une communauté.

Exemples

Des dizaines d'insultes sous votre vidéo devenue virale, c'est une agression.

Vous menacer d'abus sexuel ou de viol, c'est une agression.

Vous menacer à cause des opinions que vous avez exprimées dans un article, c'est une agression.

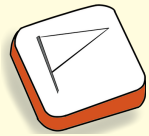
Vous inciter à quitter un jeu en ligne en disant que vous êtes nulle car vous êtes une femme, c'est une agression.

VERSO : STRATÉGIES DE RÉSISTANCE →

LES AGRESSIONS EN LIGNE

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Se déconnecter ;



Signaler ;

Couper le son ;

Jouer en équipes non mixtes.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LE GASLIGHTING

Qu'est-ce que c'est?

C'est quand on vous cache ou que l'on déforme des informations pour vous faire croire que vous vous trompez.

Vous êtes victime de gaslighting si on essaie de vous persuader que vous avez fait ou dit quelque chose alors que c'est faux.

En ligne, c'est quand on fait douter les internautes en changeant vos paroles ou vos histoires.

L'objectif est de justifier la violence envers vous et vous décrédibiliser.

Exemples

Sortir une phrase de son contexte en faisant un montage vidéo pour vous discréditer, c'est du gaslighting.

Répondre à votre témoignage d'agression sexuelle en disant que c'est exagéré ou que c'était désiré, c'est du gaslighting.

Vous dire que vous êtes hystérique quand vous dénoncez les insultes reçues en ligne, c'est du gaslighting.

Nier publiquement votre orientation sexuelle et le justifier par des mensonges, c'est du gaslighting.

VERSO : STRATÉGIES DE RÉSISTANCE →

LE GASLIGHTING

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Bloquer ;

Modifier le genre perçu du profil ;

Ignorer ;

S'entraider dans un groupe de soutien.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LE HARCÈLEMENT EN LIGNE

Qu'est-ce que c'est?

C'est vous insulter, écrire ou diffuser des obscénités ou des menaces contre vous à plusieurs reprises.

L'objectif peut être de vous faire peur, de vous intimider, de dégrader vos conditions de vie ou de vous pousser à céder sur quelque chose que vous refusez.

Exemples

Recevoir des invitations insistantes pour avoir un rendez-vous avec vous alors que vous avez déjà dit non, c'est du harcèlement.

Subir des insultes ou des menaces dès que vous gagnez dans des jeux en ligne, c'est du harcèlement.

Recevoir des messages à caractère sexuel par un ami d'ami dans un réseau social, sans votre consentement, c'est du harcèlement.

Vous humilier par des commentaires, publics ou privés, parce que vous êtes une personne médiatique, c'est du harcèlement.

VERSO : STRATÉGIES DE RÉSISTANCE →

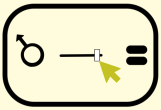
LE HARCÈLEMENT EN LIGNE

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Modération par les proches ;

Masquer ;

S'anonymiser ;



Jeux non sexistes.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

LA SEXTORSION

Qu'est-ce que c'est?

C'est menacer de diffuser des contenus intimes de vous (images, vidéos, audios, etc.).

L'objectif est de vous soutirer de l'argent, d'autres images intimes ou des faveurs sexuelles.

Exemples

Menacer de partager une vidéo intime si vous n'envoyez pas une photo de vous dénudée, c'est de la sextorsion.

Vous demander de l'argent pour ne pas révéler les images intimes de votre meilleure amie, c'est de la sextorsion.

Faire un montage de votre visage sur un corps dénudé, puis menacer de le partager si vous ne répondez pas aux messages, c'est de la sextorsion.

Menacer de diffuser des images de vos relations intimes pour vous forcer à rester en couple, c'est de la sextorsion.

VERSO : STRATÉGIES DE RÉSISTANCE →

LA SEXTORSION

EXEMPLES DE STRATÉGIES DE RÉSISTANCE :

Partager ses expériences ;

Masquer ;

Dénoncer l'adversaire ;

Quitter.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

2.CYBERASTUCES

Appareils connectés

Vérifiez les paramètres de vos appareils :

Faites un NIP fort, avec des chiffres aléatoires.
Vérifiez vos paramètres de localisation : votre historique de trajets est souvent conservé automatiquement, mais on peut vider cet historique.

Utilisez un cache caméra :

La caméra d'un ordinateur peut être piratée pour filmer à votre insu, même quand vous ne l'utilisez pas. Pensez à la masquer!

Vérifiez si vos photos sont sauvegardées dans votre appareil ou dans le nuage :

Si vos photos sont en ligne, protégez-les avec un identifiant unique et un mot de passe fort. Placez vos photos intimes dans un dossier séparé et protégé par un mot de passe fort.

Utilisez un Réseau Privé Virtuel (RPV) :

En masquant votre adresse IP, le RVP (ou VPN en anglais) vous permet de garder votre emplacement secret.

Comptes en lignes

Choisissez un mot de passe robuste :

Au moins 8 caractères, des lettres majuscules, des lettres minuscules, des caractères spéciaux et des chiffres.
Si besoin, changez l'adresse courriel de connexion à vos comptes.

Vérifiez les paramètres de vos comptes en ligne :

Pensez à tous vos comptes : courriel, comptes bancaires, sites d'achat, comptes de loisirs (Netflix, Apple TV, etc.)
Vérifiez vos paramètres de localisation : par exemple, l'historique de vos emplacements est souvent conservé automatiquement, mais on peut vider cet historique.

Désactivez l'enregistrement automatique de vos informations personnelles :

La plupart des comptes en ligne sauvegardent votre adresse, vos informations de paiement et votre historique de navigation. Vérifiez ces paramètres si vous ne voulez pas les utiliser.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

Comptes de réseaux sociaux

Choisissez un mot de passe robuste :

Au moins 8 caractères, des lettres majuscules, des lettres minuscules, des caractères spéciaux et des chiffres.
Si besoin, changez l'adresse courriel de connexion à vos comptes.

Vérifiez les paramètres de vos comptes de réseaux sociaux :

Confidentialité, localisation, géolocalisation, options de partage (public ou privé).

Désactivez la géolocalisation sur vos comptes de réseaux sociaux :

Certains réseaux sociaux proposent de vous localiser en temps réel et d'afficher votre localisation aux autres usagères et usagers. Si vous ne souhaitez pas être localisable en temps réel.

Publiez le moins d'informations personnelles ou corporatives possibles :

Gardez secrètes votre adresse courriel, votre destination de vacances, votre adresse postale, etc.

En cas d'attaque

Ces conseils ont été élaborés avec la clinique de cybercriminalité de l'UdeM.

- **Essayez de vous entourer de personnes de confiance pour ne pas vivre cette épreuve seule.**
- **Adressez-vous aux ressources d'accompagnement, d'aide psychologique ou juridique qui sont dans votre région.**
- **Bloquez les profils qui envoient des contenus agressifs, ou limitez les interactions.**
- **Signalez les personnes malveillantes et leurs agressions auprès du réseau social ou de la plateforme.**
- **Gardez une trace des agressions reçues (ex: photo, sauvegarde de la page, une capture d'écran, avec la date et l'heure de publication) :**
  Elles pourront servir de preuve en cas de dénonciation aux autorités.
- **Pour limiter l'impact des propos diffamatoires sur votre réputation :**
  Prévenez vos proches ou vos contacts professionnels si des informations jugées diffamatoires sont diffusées à votre sujet afin de les informer et d'obtenir de l'aide.
- **Gardez une trace de vos partages :**
  Conservez un historique de ce que vous avez partagé et avec qui.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

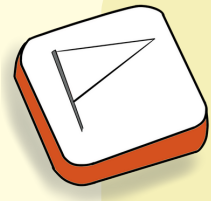
3.STRATÉGIES DE RÉSISTANCE

STRATÉGIES DE RÉSISTANCE

SE DÉCONNECTER

Lorsque c'est possible, se déconnecter de l'application permet de prendre une pause et de reprendre des forces.

SIGNALER



Avertir l'application des comportements inappropriés d'une personne peut amener les gestionnaires à prendre des mesures (suspendre le compte fautif, suppression des messages d'attaque, etc.).

RENCONTRER LES AUTORITÉS

La cyberintimidation est illégale au Canada. Si elles le souhaitent, les victimes peuvent envisager une procédure judiciaire contre leurs adversaires en ligne.

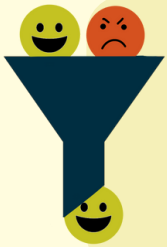
PROTÉGER SA VIE PRIVÉE

Paramétrer les informations publiques ou privées peut permettre de limiter l'accès à ses données personnelles.

MODIFIER LE GENRE PERÇU

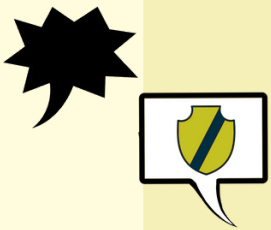
Des personnes victimes de discrimination fondée sur le genre utilisent parfois un nom ou une photo qui semblent appartenir à un homme cisgenre pour essayer de limiter les attaques, notamment sexistes.

UTILISER LA MODÉRATION AUTOMATIQUE



Selon la plateforme, on peut bloquer, masquer ou supprimer les messages violents grâce à des applications de filtres automatiques, qui analysent les textes et les images pour repérer les contenus malveillants.

RÉPONDRE



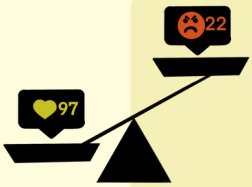
Face à l'hostilité en ligne, certaines personnes préfèrent répondre. Elles répondent parfois seules. D'autres fois, c'est un groupe de personnes qui s'allient à la victime afin de répondre à plusieurs aux attaques reçues. Plusieurs stratégies de réponse sont employées, comme répondre directement aux commentaires, détourner la conversation, etc.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF



AIMER LES COMMENTAIRES

Aimer le ou les commentaires d'une victime d'agression en ligne permet de montrer son soutien. Certaines personnes alliées iront jusqu'à répondre à l'adversaire afin de le distraire et offrir du répit à la victime.

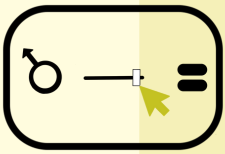
MASQUER

Cette fonction est utilisée pour cacher un message sans le supprimer, ce qui permet de garder des preuves de l'agression.

S'ENTRAIDER DANS DES GROUPES DE SOUTIEN

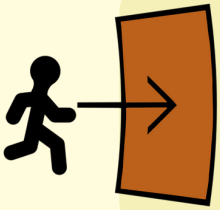
Rejoindre des groupes formels ou informels sur les réseaux sociaux, construits par les communautés elles-mêmes, peut permettre d'accéder à des espaces sûrs qui permettent d'exprimer ses émotions, d'avoir de l'écoute et de recevoir du soutien.

CHOISIR DES JEUX NON SEXISTES



Pour éviter les environnements de jeux potentiellement toxiques, il arrive que des joueuses en ligne repèrent les jeux stéréotypés ou problématiques et choisissent d'autres jeux qu'elles jugent plus éthiques ou plus sécuritaires pour elles.

QUITTER



Dans certains cas, la solution choisie est d'arrêter d'utiliser les plateformes où on subit des agressions.

PARTAGER SES EXPÉRIENCES

Échanger avec ses collègues, ses proches ou sur des groupes de soutien au sujet des agressions subies permet de partager des stratégies et de se protéger mutuellement.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

BLOQUER

Cette fonction est utilisée pour empêcher l'adversaire de nous contacter ou d'interagir avec nos publications. On peut ainsi publier sans risquer de recevoir des commentaires inappropriés du compte bloqué.

S'ANONYMISER

Utiliser une photo impersonnelle (paysage, dessin, etc.) et un nom d'emprunt permet d'être moins identifiable. On peut aussi utiliser un réseau privé virtuel (VPN) pour masque son adresse IP ou d'autres fonctionnalités pour limiter le suivi de ses activités en ligne et hors ligne.

JOUER EN ÉQUIPES NON MIXTES

Pour essayer de limiter les violences sexistes vécues, ou pour se créer des espaces de jeu plus sécuritaires, certaines personnes créent des groupes en non mixité de genre. Exemple: une équipe uniquement composée de femmes.

DÉNONCER L'ADVERSAIRE

Identifier publiquement l'adversaire dans des groupes de soutien peut permettre aux autres membres du groupe de faire preuve de vigilance par rapport à cet adversaire et de prendre des mesures pour se protéger.

CRÉER DEUX PROFILS

Quand on exerce une profession publique, avoir un compte personnel et un compte professionnel permet de limiter les intrusions dans sa vie privée, surtout si le compte personnel utilise un pseudonyme.

IGNORER

Il s'agit de ne pas ouvrir les messages de l'adversaire et de mettre en sourdine les notifications relatives à ses messages ou commentaires.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

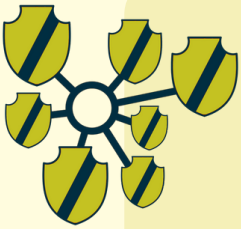
CDEACF

MODÉRATION PAR UN PROCHE

Il s'agit de demander à une ou plusieurs personnes proches de lire et prendre actions sur les commentaires et messages reçus par la personne vivant de la violence afin d'alléger sa charge mentale.

COUPER LE SON

Dans une séance de jeu en ligne, la conversation entre joueuses et joueurs peut être vocale ou écrite. Certaines joueuses choisissent de désactiver le son et les modules de clavardage pour jouer sans être contactées ou pour couper les échanges en cas de violence ou commentaires déplacés reçus.



MOBILISER UNE COMMUNAUTÉ D'ALLIÉ-E-S

En s'organisant à plusieurs, des internautes veulent parfois utiliser la force du groupe pour augmenter l'impact d'une action. Par exemple, pour signaler un adversaire et accélérer l'intervention des gestionnaires de la plateforme.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

Créez votre nétiquette en 4 questions clés

Où allez-vous diffuser cette nétiquette?

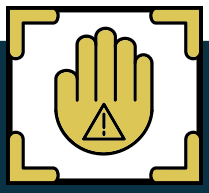
Pensez d'abord au contexte de diffusion. Est-ce sur un site web? Sur les réseaux sociaux? À la radio? Dans un épisode de baladodiffusion? Ou bien lors d'un appel téléphonique? Vous pourrez ainsi adapter la longueur et le format de présentation de votre nétiquette.

À qui vous adressez-vous?

Identifiez votre public cible, pensez aux personnes qui vont consulter votre nétiquette. Pensez particulièrement aux enjeux que peut rencontrer le public visé : accessibilité universelle, littératie numérique, alphabétisation, etc.
Cette réflexion vous permettra de formuler votre message de manière simplifiée. Votre public cible pourra donc se l'approprier plus facilement.

ENSEMBLE CONTRE l'intimidation
Avec la participation financière de : Québec
CDEACF Centre de documentation sur l'éducation des adultes et la condition féminine

Créez votre nétiquette en 4 questions clés



Quel est le message que vous souhaitez faire passer?

Voulez-vous rappeler l'objectif de l'espace d'échange que vous animez? Voulez-vous avertir des actions entreprises en cas d'enfreinte à la nétiquette formulée? Donnez des indications claires à votre public cible. Par exemple : « nous allons signaler les courriels contenant des message haineux ».
Formuler des informations claires permet notamment d'amener vos interlocuteurs à réfléchir sur l'objectif de cette nétiquette et à comprendre les règles auxquelles ils souscrivent.

Comment souhaitez-vous diffuser l'information?

Pensez-vous rédiger vos règles de nétiquette sous forme de paragraphe sur une page? Allez-vous enregistrer un message oral? Envisagez-vous d'utiliser un format multimédia? Quel que soit le format choisi, vérifiez qu'il soit accessible et adapté au contexte de votre activité. C'est d'autant plus important si vous créez des contenus multimédia, comme des vignettes, des images ou des capsules audio-vidéo.
Diffuser vos mesures de nétiquette de manière adaptée et accessible en facilitera la consultation.

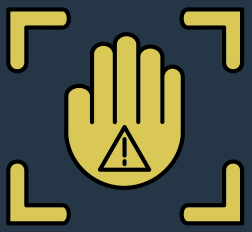
ENSEMBLE CONTRE l'intimidation
Avec la participation financière de : Québec
CDEACF Centre de documentation sur l'éducation des adultes et la condition féminine

Créez votre nétiquette en 4 questions clés

Où allez-vous diffuser cette nétiquette?

À qui vous adressez-vous?

Quel est le message que vous souhaitez faire passer?



Comment souhaitez-vous diffuser l'information?

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF
Centre de documentation
sur l'éducation des adultes et la condition féminine