Promotion - Santé / Bien-être / Questions psychosociales

Harcèlement par Internet ou cyberharcèlement

Sur cette page

Pourquoi un employeur devrait-il se pencher sur le harcèlement par Internet?

De nombreux travailleurs utilisent un ordinateur ou l'Internet dans le cadre de leur travail. Le harcèlement par Internet est considéré comme un problème au travail, ainsi qu'à la maison et à l'école.

Veuillez consulter les fiches d'information Réponses SST suivantes pour plus d'information :

- Intimidation en milieu de travail
- Harcèlement par Internet ou cyberharcèlement
- Violence et harcèlement en milieu de travail
- Violence et harcèlement en milieu de travail – Violence familiale
- Violence et harcèlement en milieu de travail – Législation
- Violence et harcèlement en milieu de travail – Gérer les interactions négatives
- Violence et harcèlement en milieu de travail – Sécurité dans les parcs de stationnement

- Violence et harcèlement en milieu de travail – Signes précurseurs
- Violence et harcèlement en milieu de travail – Travailler tard

Quels sont des exemples de harcèlement par Internet ou de cyberintimidation?

Le harcèlement par Internet, aussi appelé « cyberintimidation », consiste en l'utilisation du réseau Internet pour intimider, harceler, menacer ou embarrasser quelqu'un de façon malicieuse. Ce type de harcèlement peut se manifester sous diverses formes :

- Transmission de courriels non sollicités et/ou menaçants.
- Incitation de tierces personnes à transmettre à la victime des courriels non sollicités et/ou menaçants ou à surcharger cette dernière par un très grand nombre de messages électroniques.
- Transmission de virus par courrier électronique (sabotage électronique).
- Diffusion de rumeurs.
- Transmission en ligne de commentaires diffamatoires au sujet de la victime.
- Transmission de messages négatifs directement à la victime.
- Utilisation en ligne de l'identité de la personne pour transmettre un message controversé, offensant ou injurieux qui suscitera chez de tierces personnes une réponse négative à la victime ou une réaction défavorable à son égard.
- Harcèlement de la victime pendant une discussion en direct.
- Enregistrement en ligne de messages abusifs, y compris les sites de médias sociaux.
- Transmission à la victime de documents pornographiques ou autres matériels graphiques à caractère offensant.
- Création de contenus en ligne qui représente la victime de manière négative.

Que peut-on faire pour prévenir le cyberharcèlement?

Bien que chaque situation soit différente, en général, les mesures à prendre pour prévenir la cyberintimidation peuvent comprendre les suivantes :

Sur le lieu de travail :

- Utiliser une adresse électronique sans distinction de sexe, dans la mesure du possible.

- Utiliser un mot de passe électronique composé d'au moins douze (12) caractères, bien qu'il puisse être approprié de choisir des mots de passe plus longs. S'assurer qu'il s'agit d'une combinaison de lettres minuscules et majuscules, des chiffres, et des symboles. Les meilleurs mots de passe ne veulent rien dire et ne sont pas formés selon une séquence logique.
- Changer régulièrement son mot de passe.
- Passer en revue la politique du lieu de travail concernant l'utilisation des signatures de courriel (le bloc de texte qui est ajouté automatiquement à la fin d'un message sortant). Il doit fournir suffisamment de renseignements sur la personne pour qu'elle puisse être identifiée, mais pas au point de fournir des renseignements personnels aux destinataires des courriels.
- Utiliser le chiffrement, les paramètres de confidentialité, un logiciel ou d'autres outils technologiques pour rendre plus sûre l'utilisation des courriels et d'Internet.
- Suivre les lignes directrices du spécialiste de la technologie Internet de votre organisation, car il y aura des exigences supplémentaires concernant les paramètres de confidentialité et la protection contre les virus informatiques, les logiciels malveillants, etc.
- Suivre toutes les politiques ou procédures mises en place par votre organisation pour les communications par Internet. Discuter de la confidentialité et de la sécurité sur Internet avec le spécialiste de la technologie Internet de votre organisation.
- Limiter les renseignements que vous communiquez dans votre avis d'« absence du bureau » aux dates de votre absence et aux personnes à joindre. Ne pas faire savoir à tout le monde que vous êtes en vacances ou en déplacement pour des raisons professionnelles.
- Ne pas laisser votre ordinateur connecté et sans surveillance.

Autres conseils :

- Faire attention à ce que vous publiez. Bien que vous puissiez supprimer le message d'origine, il n'est pas possible de supprimer les copies que d'autres ont faites.
- Demeurer attentif aux questions pièges, c'est-à-dire aux personnes qui demandent de l'information sur son adresse à domicile ou son lieu de travail.
- Demeurer prudent avant de rencontrer en personne des gens connus seulement via l'Internet. Dans l'éventualité d'une rencontre en personne, choisir un endroit public et se présenter en compagnie d'un ami ou un collègue de travail.
- Envisager de créer à des fins personnelles deux comptes de courriel : un qui sera utilisé pour la correspondance officielle et le deuxième, enregistré sous un nom fictif, pour les groupes de discussion, etc. Si trop de courriels non sollicités sont envoyés à cette deuxième adresse, la modifier ou l'annuler complètement.

- Pour conserver l'anonymat, NE PAS enregistrer son adresse électronique sur aucune page Web ni sur un formulaire mémorisé dans une page Web à moins que cela ne soit nécessaire.
- Si possible, utiliser un navigateur anonyme pour naviguer sur le Web. Les sites Web consignent des renseignements au sujet de leurs visiteurs (par exemple le fureteur utilisé, « témoins », le fournisseur de service Internet utilisé et même l'adresse électronique utilisée). Les fureteurs anonymes offrent des degrés divers de sécurité, certains d'entre eux peuvent être utilisés sans frais et d'autres, pas.
- Discuter avec le fournisseur de service Internet de l'importance accordée à la confidentialité et la sécurité en ligne. Obtenir les conseils et l'assistance du fournisseur de service Internet au besoin.
- Vérifier que le fournisseur de service Internet ainsi que les groupes de discussion et les réseaux de débat public utilisés ont adopté une politique de savoir-vivre en réseau (qui interdit le harcèlement) et que cette politique est mise en application par le gestionnaire du site Web.

À ÉVITER

- Ne pas divulguer son mot de passe à qui que ce soit.
- Ne pas fournir de renseignements personnels dans ses courriels – pas même dans un message transmis à une personne en qui on a confiance.
- Ne pas partager de renseignements personnels dans des forums publics où que ce soit en ligne et ne pas les donner à des inconnus, y compris dans les clavardoirs.
- Ne pas affronter ni insulter qui que ce soit en participant à un groupe de débat public. En cas de désaccord, décrire simplement les faits et énoncer sa position de façon objective.

Comment devez-vous agir si une personne vous harcèle par courriel?

Si la personne fait partie de votre lieu de travail :

- Signaler le ou les incidents en suivant la politique et les procédures de votre lieu de travail en matière d'intimidation, de harcèlement, ou de violence au travail.

Si une personne vous harcèle par courriel (en général) :

- Si le harceleur est connu, lui dire en termes très clairs que vous ne voulez plus qu'il communique avec vous.

- Une fois que vous avez dit au harceleur que vous connaissez de ne plus communiquer avec vous ou encore si vous recevez une profusion de courriels d'un inconnu, faire intercepter ou filtrer les messages provenant de cet abonné. De nombreux programmes de messagerie ont une fonction de filtre qui permet de supprimer ou de déplacer automatiquement les courriels provenant d'une adresse électronique particulière ou contenant des mots blessants dans un dossier distinct.
- NE PAS répondre à un courriel offensant, non sollicité ou provenant d'un harceleur que vous ne connaissez pas. En répondant à un tel message, vous confirmez que votre adresse électronique est valide et toujours utilisée.
- NE PAS ouvrir les fichiers joints. Ces derniers pourraient contenir des virus.
- Consigner les actes de harcèlement dans un registre. Sauvegarder, en guise de preuve, toutes les communications injurieuses ou offensantes à la fois en versions électronique et imprimée. Ne PAS modifier ni réviser ces communications d'aucune façon.
- En utilisant votre nom, effectuer une recherche sur le Web pour savoir s'il existe des informations sur vous. Ainsi, vous serez au courant de la nature des informations sur vous qui sont disponibles au public.
- Si vous connaissez la personne qui vous harcèle et qu'elle continue de vous harceler après que vous lui ayez demandé de cesser, communiquer avec le fournisseur de service Internet du harceleur :
    - La plupart de ces fournisseurs ont adopté des politiques précises interdisant l'utilisation de leurs services en vue d'importuner ou de harceler une autre personne.
    - Le fournisseur de service Internet est souvent en mesure de stopper de tels actes en communiquant directement avec le harceleur ou en mettant fin à son abonnement.
    - Le nom de domaine du fournisseur de service est identifié par l'information qui suit le @ (p. ex. nom@résidence.com). La plupart des fournisseurs ont une adresse électronique du type webmestre@nomdedomaine, où vous pourrez enregistrer une éventuelle plainte.

Que pouvez-vous faire si une personne vous harcèle publiquement (dans un groupe de discussion ou pendant une séance de clavardage)?

Si quelqu'un vous harcèle dans un groupe de discussion :

- Consigner les actes de harcèlement dans un registre.

- Sauvegarder, en guise de preuve, toutes les communications injurieuses ou offensantes à la fois en versions électronique et imprimée. NE PAS modifier ni réviser ces communications d'aucune façon.
- Communiquer avec le gestionnaire du groupe et lui transmettre les preuves de ce harcèlement. S'il ne répond pas, se retirer de ce groupe (c.-à-d. faire supprimer son adresse électronique de la liste de diffusion du groupe).

Si quelqu'un vous harcèle sur un site de bavardage en ligne :

- Quitter le réseau. Si la situation met votre sécurité ou celle des autres en péril, communiquer avec le service de police ou un organisme d'application de la loi de votre région.
- Conserver un dossier pour toute activité liée au harcèlement.
- Consigner les actes de harcèlement dans un registre.
- Sauvegarder, en guise de preuve, toutes les communications injurieuses ou offensantes à la fois en versions électronique et imprimée. NE PAS modifier ni réviser ces communications d'aucune façon.
- Communiquer avec le responsable du groupe et lui transmettre les preuves de ce harcèlement. S'il ne répond pas, cesser de participer aux débats de ce groupe.

Que devez-vous faire si quelqu'un vous intimide ou vous harcèle sur des sites de médias sociaux?

La plupart des applications (« apps ») et des sites de médias sociaux (comme Facebook, Twitter, YouTube et Snapchat) ont publié des directives sur ce qui devrait et ne devrait pas être publié sur leurs sites. Ces lignes directrices sont habituellement disponibles sous la rubrique « Modalités d'utilisation » ou « Normes/lignes directrices de la communauté ». Ces sites disposent aussi d'un mécanisme pour signaler des abus en lien avec ces lignes directrices. Au moment de formuler une plainte, nous vous suggérons de recourir aux conseils susmentionnés pour documenter la situation. Avant de soumettre votre rapport, assurez-vous de joindre au dossier une capture d'écran d'un commentaire ou une copie d'une photo comme éléments de preuve. Si vous pensez être en danger immédiat, communiquez avec la police localel ou un organisme d'application de la loi.

En tant qu'utilisateur, vous pouvez toujours décider de prendre des mesures comme :

- Penser avant d'afficher – ces mots ou cette photo peuvent-ils être vus par tout le monde? Vos commentaires pourraient-ils susciter une réaction potentiellement dangereuse?
- Utiliser les paramètres de confidentialité recommandés fournis par le site.

- Supprimer, cacher, bloquer ou désactiver un autre utilisateur afin qu'il ne voit pas votre profil.
- Supprimer les commentaires sur les messages ou les photos, ou ajuster vos paramètres de confidentialité afin d'être en mesure d'examiner les commentaires avant de les publier.
- Garder les renseignements personnels privés, y compris votre adresse, date de naissance, numéro de téléphone, degré de scolarité, numéros de carte de crédit et mots de passe. Être au fait des détails que vous montrez dans les photos, comme le numéro d'adresse civique, les noms des rues, les lieux de travail.
- Désactiver les paramètres de localisation qui peuvent être intégrés à votre appareil lors de la prise de photos.
- Fermer les sessions sur vos comptes lorsque vous avez terminé. Plus particulièrement, si vous utilisez un ordinateur ou un dispositif public.
- Éviter les représailles. La plupart des intimidateurs cherchent à obtenir une réaction.

Comment NE PAS agir si une personne vous harcèle par courriel?

NE PAS transmettre de message ni répondre à un courriel lorsque vous êtes en colère ou contrarié. Attendre de retrouver son calme; vous ne voudriez pas être perçu comme le harceleur.

NE PAS se laisser entraîner dans un affrontement. Vous risquez de déclencher une « flambée » qui peut s'aggraver rapidement.

NE PAS répondre à une flambée d'insultes (provocation en ligne).

NE PAS poursuivre les échanges du type questions et réponses qui vous rendent mal à l'aise.

(Tiré du guide Prévention de la violence en milieu de travail du CCHST)

Date de la dernière modification de la fiche d’information : 2020-12-23

Avertissement