APTE-Sénégal

Projet d'Amélioration des Performances de Travail et d'Entreprenariat au Sénégal

Module 8 : Culture numérique

Guide de l'élève du Collège d'Enseignement Moyen

Module 8 : Culture numérique.

Bu jamono sopeekoo, dangay sopeeku and ak moom ci lu baax »
(Quand le monde change, il faut changer avec positivement)

Objectifs de la culture numérique :

À la fin du module, les élèves seront capables de:

- ✓ Identifier les moyens de créer une présence en ligne ;
- ✓ Identifier les bonnes pratiques en matière de sécurité lorsqu'on est en ligne pour se protéger contre les pirates informatiques, les escrocs, la Cyberintimidation etc. ;
- ✓ Utiliser efficacement les ressources en ligne pour trouver du travail.

Aperçu du module 8

✍Activité
Séance 1 : Création de sa propre présence en ligne
1 : Introduction à la culture numérique et à la présence en ligne (y compris l'autoévaluation)
2 : Types de présence en ligne
3 : Étapes de la création d'une présence en ligne
4 : Créer une adresse email
Séance 2 : Citoyenneté numérique
5 : Sécurité numérique
6 : Cyberintimidation, trolling et cyberprédateurs /cyberprédatrices
7 : Directives générales pour être un(e)cybercitoyen(ne)
Séance 3 : Chercher des ressources en ligne
8 : Mettre en doute les informations fournies en ligne
9 : Améliorer ses recherches sur le Net
10 : Aider les utilisateurs/utilisatrices à vous trouver sur le Net

Documents à l'intention des élèves

- ❑ 8.7: Est-ce que *vous* vous comportez comme un cyberintimidateur / une Cyberintimidatrice ?

Autoévaluation initiale
Module 8 : Culture numérique

Il n'y a ni bonnes ni mauvaises façons de répondre à cette activité d'autoévaluation. Nous voulons juste recueillir vos manières de penser et de faire pour nous aider à mieux dérouler ce qui va suivre. Ceci servira également à votre usage personnel lors de ce cours. Le professeur/la professeure va lire une compétence énumérée dans la colonne de gauche.
Lisez les choix dans la partie supérieure. En pensant à vous-même, dites quel point représente le mieux votre situation en cochant la case correspondante dans chaque colonne. À la fin de ce module, nous répéterons cette évaluation.

Mon expérience **Connaissances, compétences et capacités**	**(1)** **Je n'ai aucune connaissance à ce sujet**	**(2)** **J'ai peu de connaissances à ce sujet**	**(3)** **J'ai quelques connaissances à ce sujet pour parfois le faire correctement**	**(4)** **J'ai beaucoup de connaissances à ce sujet et je peux le faire régulièrement**	**(5)** **J'ai beaucoup de connaissances à ce sujet et je peux le faire correctement et de façon consistante**
Créer une présence en ligne par email et par les plates-formes de réseaux sociaux telles que Facebook, YouTube, etc.,					
Déterminer les moyens par lesquels je peux présenter en ligne mes compétences, aptitudes, expériences et intérêts					
Consulter et analyser la présence en ligne de certaines personnes pour identifier les éléments de succès et stratégies de présentation en ligne					

Mon expérience Connaissances, compétences et capacités	(1) Je n'ai aucune connaissance à ce sujet	(2) J'ai peu de connaissances à ce sujet	(3) J'ai quelques connaissances à ce sujet pour parfois le faire correctement	(4) J'ai beaucoup de connaissances à ce sujet et je peux le faire régulièrement	(5) J'ai beaucoup de connaissances à ce sujet et je peux le faire correctement et de façon consistante
Identifier comment utiliser une présence en ligne pour trouver de l'emploi ou développer ma propre entreprise					
Faire usage des pratiques de sécurité lorsque je suis en ligne pour me protéger contre les pirates informatiques, les escrocs, etc.					
Reconnaitre la cyberintimidation, y compris l'humiliation et l'agression					
Prendre une position proactive contre la cyberintimidation					
Utiliser la pensée critique pour analyser des ressources en ligne (qui envoie, pourquoi, source de l'information, etc.)					
Chercher efficacement des ressources en ligne					
Utiliser des ressources en ligne pour trouver du travail					

Séance 1 : Création de sa propre présence en ligne.

🗝 Sujets clés 🗝

- Types de présence en ligne ;
- Traits principaux et bonnes stratégies de présence en ligne ;
- Se présenter personnellement et professionnellement en ligne ;
- Étapes de la création d'une présence en ligne ;
- Étapes de la création d'un compte email.

8.1: Différents types de médias sociaux[7] :

[7] Tiré et adapté de: https://www.cite.co.uk/the-different-types-of-social-media/le 22 Octobre 2015.

Les médias sociaux incluent la technologie qui encourage les utilisateurs/utilisatrices à interagir les un (e)s avec les autres en créant et échangeant le contenu qu'ils/elles ont produit. En outre, les fonctions et dimensions peuvent être très différentes. Quelques-unes des plates-formes les plus populaires sont devenues une combinaison de plusieurs de ces catégories. Les principales catégories de médias sociaux sont :

Réseaux sociaux : un service en ligne, une plate-forme ou un site web qui permet aux utilisateurs/utilisatrices de créer leur propre profil et de développer des relations avec les autres utilisateurs/utilisatrices. Les interactions sur ces sites créent des communautés en ligne où les gens échangent fréquemment des informations à travers des publications, liens, photos, vidéos et autres multimédias. Les exemples très connus sont Facebook, Google+ et LinkedIn ;

Blogs : abréviation de « web log », un blog est un site web (ou partie d'un site web) où des articles sont écrits et publiés pour que les gens puissent les lire. Souvent, les gens peuvent laisser des commentaires en bas de la publication pour encourager les échanges ;

Microblogs : Version plus courte d'un blog, les microblogs permettent aux auteurs de partager des informations rapides au lieu de longs articles. Il s'agit des sites comme Twitter, qui limite les publications à 140 caractères, Posterous et Tumblr. Les microblogs ne reposent pas toujours sur des textes. En effet, Pinterest rassemble des gens qui partagent principalement des images ou des vidéos ;

Évaluations en ligne : Quiconque prévoit de faire un voyage ou a besoin d'informations concernant les restaurants locaux aura probablement à chercher à travers les sites d'évaluation en ligne comme TripAdvisor, Zagat ou Google. Les sites d'évaluation en ligne permettent aux gens de laisser des critiques à propos d'un endroit, hôtel, restaurant ou autres prestations spécifiques de sorte que d'autres personnes peuvent avoir une idée du service auquel s'attendre. Cet attribut est aussi populaire dans les sites de commerce électronique, tels qu'Amazon et eBay, puisque plusieurs personnes consultent les remarques/commentaires des autres à propos d'un produit avant de l'acheter ;

Partage de signets (social bookmarking) : Les sites de partage de signets permettent aux utilisateurs/utilisatrices de sauvegarder et partager leurs sites web favoris. Les utilisateurs/utilisatrices peuvent aussi évaluer ces sites, les étiqueter par catégories et laisser des commentaires. À travers ce processus, les sites peuvent être recommandés aux autres, ce qui par conséquent augmente la visibilité de ceux-ci et aide les gens à avoir accès au contenu qui les intéresse. Les sites de partage de signets populaires sont StumbleUpon, Del.icio.us et Digg ;

Web audio (podcasts) : Les Podcasts sont généralement des fichiers audios ou des vidéos publiés en ligne que les gens peuvent télécharger ou garder sur un ordinateur ou autre appareil (téléphone) mobile. Les Podcasts ont obtenu leur nom en combinant « broadcast » (émettre) et « pod », ce qui fait référence à leur popularité par les « utilisateurs/utilisatrices d'iPod » ;

Les forums /mur : L'un des plus vieux types de média social, les forums permettent aux utilisateurs/utilisatrices d'échanger sur un sujet spécifique. Les gens peuvent poser des questions ou participer à une conversation spécifique en ligne. Exemple : le forum de seneweb ;

Connaissances sociales/Wikis : Ces sites contiennent des contenus amenés par les utilisateurs eux-mêmes/utilisatrices elles-mêmes pour créer un centre de connaissances auquel les autres peuvent se référer. Quelques-uns de ces sites, tels que Wikipedia, Answers.com et Quora, sont grands et peuvent être accédés par le public alors que d'autres peuvent être limités à un groupe de gens faisant partie d'une même organisation ;

Géolocalisation : Ce type de média social consiste à déterminer la localisation de l'utilisateur/utilisatrice et est souvent associé aux appareils/téléphones mobiles. Les plates-formes de géolocalisation permettent aux utilisateurs/utilisatrices de s'enregistrer (check-in) à l'endroit où ils/elles se trouvent et localiser des ami(e)s se trouvant dans les environs. (Ex : FourSquare) ;

Multimédias : Les utilisateurs/utilisatrices de ces sites s'en servent principalement pour échanger des multimédias tels que des vidéos, photos, images infographiques et PDFs. Les gens peuvent habituellement laisser des commentaires et partager le contenu avec d'autres personnes. Les exemples connus sont YouTube, Instagram (site de photos) et Snapchat.

8.2: Création de votre présence en ligne :

1. Stratégies : Quels sont vos objectifs ?

Pensez à vos objectifs à court et à long terme. Vous pouvez chercher à obtenir des informations sur une école ou un emploi. Vous pouvez vouloir commencer votre propre entreprise. Comment est-ce que la création d'une présence en ligne vous aidera à atteindre vos objectifs ?

2. Créer une plate-forme solide :

Pour la plupart des petites entreprises et des entrepreneur(e)s, la création d'une plate-forme solide commence avec la création d'un groupe ou d'une page sur un réseau social (WhatsApp, Facebook, Messenger…). Pour ceux et celles qui cherchent de l'emploi, vous pouvez envoyer un email incluant un cv ou une lettre de demande d'emploi.

Pour ceux qui créent un groupe, un réseau ou une page, il doit s'agir d'une place où toute l'information importante y est centralisée. Les gens peuvent y consulter ce que vous avez à leur offrir et les façons de vous contacter.

Il faut absolument inclure un message compréhensible (de ce qu'est votre entreprise), une navigation facile à utiliser, une page de contact, une page à propos de vous et un bon contenu.

3. Toujours optimiser et innover :

Ne pensez pas que toute chose doit être parfaite avant de la mettre en ligne. Vous aurez toujours à améliorer votre contenu et ce que vous avez à offrir.

4. Être consistant(e) :

Que ce soit à travers votre site web une communauté en ligne ou les médias sociaux, vous devez toujours être consistant.

Quel contenu donnez-vous à votre public ?

Ce peut être un blog, des vidéos ou des produits à vendre ; peu importe la forme que prend ce contenu, assurez-vous qu'il ait de la valeur et qu'il soit consistant.

La création d'un contenu consistant et intéressant vous aidera à gagner de la crédibilité et de l'autorité dans votre industrie ou votre domaine d'expertise ; ce qui est important pour votre croissance et votre visibilité en ligne.

Ceci vous aidera à bâtir la confiance entre vous et ceux qui vous suivent et vous aidera à construire des relations avec les autres dans votre industrie ou domaine d'expertise.

5. Être sociable :

Choisissez deux ou trois réseaux sociaux qui sont les mieux adaptés à votre entreprise ou à vous personnellement si vous souhaitez vous mettre en valeur auprès d'employeurs potentiels/employeuses potentielles.

Les médias sociaux peuvent être un outil SUBSTANTIEL de marketing/publicité qui vous aident à gagner le cœur de vos principaux admirateurs. C'est aussi un outil important pour rejoindre ceux et celles qui vous connaissent déjà, qui vous aiment et qui ont confiance en vous.

6. Commencer à créer des relations :

Trouvez un groupe ou une communauté en ligne composé d'individus ayant les mêmes intérêts que les vôtres ou qui gèrent une entreprise similaire à la vôtre.

Ensuite, commencez à créer des relations avec eux en devenant un membre actif dans le groupe, en incitant le débat et en y participant.

Si vous commencez votre entreprise, il y a une forte chance que ces gens aient plus de contacts que vous et qu'ils peuvent vous introduire aux autres qui œuvrent dans votre domaine.

Il faut aussi trouver un groupe d'individus qui correspond à la description de votre public potentiel. En effet, rejoindre ce genre de communauté peut vous donner une bonne idée de leurs besoins.

Encore une fois, il faut toujours commencer par donner de la valeur aux autres. Quand vous entrez dans un groupe ou une communauté, il est important de ne PAS faire la publicité de vous-mêmes ou de votre entreprise. Une fois que vous commencerez à établir des relations solides avec les autres dans la communauté, ils/elles s'intéresseront naturellement à ce que vous faites et, avec le temps, vous pourrez commencer à partager vos informations.

8.3: Comment faire la promotion de soi-même ?

Chercher un emploi ou attirer une clientèle est semblable à quelques-uns des concepts appris lors du module sur la notion de marché :

1. **Aperçu attrayant** : Assurez-vous que ce que vous écrivez est présenté d'une façon qui capte l'œil. Utiliser beaucoup de tirets, mettre en caractères gras, etc. rendra la lecture plus facile qu'un long texte ;

2. **Compétences et aptitudes souhaitables** : Utilisez les mots clés que les employeurs/employeuses recherchent dans votre cv et lettre de motivation. Pour ce faire, observez des descriptions en ligne d'emploi dans votre domaine pour voir ce que les employeurs/employeuses exigent ;

3. **Se démarquer des autres** : Montrez aux employeurs/employeuses que vous avez les compétences qu'ils/elles recherchent et, plus encore, qui pourront les aider à surpasser leurs adversaires. Montrez à vos clients que vos produits ou services sont de la plus haute qualité ;

4. **Recommandations** : Vous avez besoin de gens qui parlent en bien de vous ou des services/produits que vous vendez ou offrez. Les employeurs/employeuses et client(e)s veulent savoir que vous faites un bon travail ;

5. **Prix compétitif :** Trouvez la valeur que vous avez sur le marché. Combien gagnent ceux qui ont une position similaire à la vôtre gagnent ? Soyez flexible et négociez.

Séance 2 : Citoyenneté numérique

🗝 Sujets Clés 🗝

- Sécurité numérique ;
- Cyberintimidation et trolling ;
- Propriété intellectuelle ;
- Conseils généraux pour être un(e) citoyen(ne) numérique.

8.4 : Sécurité en ligne[8] :

Le Net offre plusieurs opportunités d'explorer, créer et collaborer. Pour naviguer sur le web et en prendre pleinement avantage, il est important de se sécuriser. Voici quelques conseils pour ce faire :

- ✓ Sécurisez vos mots de passe : n'utilisez pas toujours le même mot de passe pour tous vos différents comptes ; créez des mots de passe complexes en utilisant des lettres, des nombres et des symboles ;
- ✓ Déconnectez-vous de tous vos comptes quand vous avez terminé de les utiliser ;
- ✓ Utilisez des réseaux sécurisés : Il faut être très prudent(e) chaque fois que vous allez en ligne utiliser un réseau que vous ne connaissez pas (n'écrivez aucune information personnelle telle que les numéros des comptes bancaires et mots de passe) ;
- ✓ Verrouillez votre écran ou appareil quand vous ne l'utilisez pas ;
- ✓ Utilisez un antivirus pour protéger votre appareil contre des logiciels malveillants (des virus conçus pour endommager votre appareil ou réseau) ;
- ✓ Suivez les procédures de sécurité d'achat en ligne :
  - Comparez le prix avec ceux d'autres détaillant(e)s pour vous assurer qu'ils sont similaires ;
  - Faites une recherche sur les vendeurs/vendeuses qui ne vous sont pas familiers/familières ;
  - Utilisez une méthode de paiement incluant des mesures de protections de l'acheteur/acheteuse (par exemple, quelques systèmes de paiement en ligne ne révéleront pas aux vendeurs/vendeuses le numéro complet de la carte de crédit) ;
  - Gardez une copie du dossier de transaction ;
  - N'entrez pas d'informations personnelles sur les sites louches ;
  - Utilisez une connexion sécurisée quand vous voulez acheter quelque chose en ligne.

[8] https://www.google.com/safetycenter/everyone/start/, accédé le 26Octobre 2015

8.5 : Piratage d'identité [9] :

Le **vol d'identité** ou piratage de compte se produit lorsqu'une personne utilise les informations personnelles d'une autre personne à des fins financières ou pour avoir de l'information. C'est illégal. Bien que nous sommes beaucoup plus complexes qu'un morceau de papier ou qu'une empreinte digitale, quand nous voulons confirmer notre identité, nous comptons sur notre accréditation – carte d'identité, certificat de naissance, carte bancaire et de crédit, permis de conduire, carte de santé et d'emploi et beaucoup d'autres formes de documents d'identification.

Avoir une présence en ligne exige que vous partagiez quelques informations personnelles. Votre tâche est de déterminer si la source qui demande vos informations personnelles est fiable et de bonne réputation :

- ✓ Faites une vérification des antécédents : cherchez l'adresse et le numéro de téléphone et appelez pour parler à un(e) représentant(e) de l'entreprise ;
- ✓ Cherchez une politique de confidentialité et examinez-la ;
- ✓ Vérifiez si le site web est crypté ou sécurisé, une autre couche de sécurité pour vous (vous serez capable de le dire à l'aide de la barre d'adresse : si l'on peut lire « http » et qu'un petit cadenas paraît au bas de l'écran ;
- ✓ Assurez-vous que vos transactions sont sécurisées ; lorsque vous avez terminé, assurez-vous de vous déconnecter, effacez votre historique ou fermez votre fenêtre avant de continuer à naviguer ;

Vol d'identité et escroquerie :
L'escroquerie en ligne a pour but d'obtenir vos informations personnelles importantes- telles que les mots de passe ou les informations concernant vos cartes de crédit et comptes bancaires- en se faisant passer pour une entreprise avec laquelle vous faites affaires et en laquelle vous avez confiance. La plupart des escroqueries se font en copiant le contenu et l'apparence de banques et de sites web de carte de crédit. On cherche à ce que vous croyiez que vous êtes tout simplement en train de mettre à jour vos informations de compte alors que réellement, vous êtes en train de les donner à un arnaqueur/une arnaqueuse. Quelques-unes de ces contrefaçons sont très convaincantes de sorte qu'il peut être difficile de distinguer l'escroquerie de la réalité. Cependant, voici quelques signes qui peuvent vous aider à identifier l'escroquerie :

- ✓ L'email ne s'adresse pas à vous personnellement, mais commence avec une ouverture générique telle que « cher client » ou « chère cliente » ;
- ✓ Le lien URL fourni apparait comme celui appartenant à une entreprise/organisation en laquelle vous avez confiance, mais lorsque vous le lisez au complet, vous vous rendez compte qu'il ne s'agit pas exactement du même que le lien réel ;
- ✓ Il y a un ton d'urgence à la demande, comme si des mesures sérieuses seront prises contre vous si vous n'y répondez pas dans l'immédiat ;
- ✓ On vous demande de soumettre des informations que l'organisation devrait déjà avoir.

[9]Taken from Taking it Global's website retrieved on October 25, 2015: https://www.tigweb.org/themes/onlinesafety/cyber_bullying_and_predators.html, retrieved on October 25, 2015

8.6: Cyberintimidation, *trolling*[10] et cyberprédateurs/cyberprédatrices[11] :

Un autre aspect de la sécurité sur le net est d'être conscient(e) de l'existence de la cyberintimidation et du *trolling*.

Trolling :

Le *trolling*, dans le jargon des internautes, désigne une personne qui, intentionnellement, commence à argumenter ou contrarier les autres en publiant des remarques provocatrices tout en restant souvent anonyme. Les commentaires sont envoyés à tous les gens, et non à une seule victime, avec le but d'obtenir leur attention. Les *trolls* font ceci pour leur propre amusement et pour :

- **Être offensif et argumentateur/offensive et argumentatrice ;**
- **Tirer du plaisir à agacer les autres ;**
- **Se sentir puissant(e) ;**
- **Gagner de la reconnaissance ;**
- **Contrarier les gens.**

Que faire en cas de *trolling* ?

Ignorer au lieu d'encourager un(e)*troll*. En d'autres termes, « S'il vous plaît, ne pas nourrir les *trolls* ».

Cyberintimidation :

La cyberintimidation vise des individus en particulier plutôt que des communautés de gens. Il s'agit d'un mal intentionnel et répété infligé en publiant des choses haineuses avec l'intention d'humilier ou intimider la victime. Ceci peut se présenter sous différentes formes, que ce soit en public ou en privé – les messages, photos, vidéos, etc. Les cyberintimidateurs/cyberintimidatrices visent à :

- Se venger ;
- Se donner du pouvoir ;
- Gagner de la popularité ;
- Harceler et menacer ;
- Être offensif /offensive ;
- Humilier ;

[10]Lohmann, RaychelleCassada, M.S., LPC, GCDF, *Trolling or Cyberbullying? Or Both?*, 28 janvier, 2014 à https://www.psychologytoday.com/blog/teen-angst/201401/trolling-or-cyberbullying-or-both

[11]Taken from Taking it Global's website retrieved on October 25, 2015: https://www.tigweb.org/themes/onlinesafety/cyber_bullying_and_predators.html, retrieved on October 25, 2015

- Intimider ;
- Contrarier la victime.

Que faire si vous êtes cyberintimidé(e) ?

- Ne répondez pas. ;
- Bloquez-la (les) personne(s). Changez votre réseau social pour éviter que la personne qui est en train de vous menacer accède à vos informations personnelles se trouvant sur votre profil. En cas de besoin, changez même votre nom d'utilisateur/utilisatrice et vos mots de passe ;
- Tenir un registre des remarques que l'on vous a faites pour vous en servir comme preuve en cas de besoin. Sauvegardez des captures d'écran, publications, etc. que vous pourrez utiliser si vous décidez de passer à la prochaine étape, c.-à-d., aller en justice ;
- Soyez sélectif/sélective à propos de ce que vous affichez. Ne publiez aucune information en ligne que quelqu'un d'autre pourrait utiliser contre vous ;
- Signalez-le : dites à un membre de la famille ou une autre personne de confiance ce qui s'est passé et comment cela vous affecte. Ensuite, informez les propriétaires des sites web/réseaux sociaux sur lesquels la cyberintimidation a eu lieu. Vous pouvez signaler les abus sur certains des réseaux sociaux les plus populaires tels que Facebook, Twitter, YouTube, Snapchat, Ask.fm, Flickr, Pinterest.

Cyberprédateurs/cyberprédatrices :

La plupart des cyberprédateurs/cyberprédatrices ont le même but : trouver une personne et l'amener à faire des actes sexuels tels que la pornographie infantile ou de réelles rencontres sexuelles. Les cyberprédateurs/cyberprédatrices aiment les défis et ne se présentent généralement pas sous leur vrai jour. Ils/elles peuvent prendre n'importe quelle identité qu'ils choisissent - homme, femme, jeune ou personne âgée - et peuvent facilement faire en sorte que l'on ait confiance en eux. Ils/elles sont intelligent(e)s, persuasifs/persuasives et implacables. Ne faites aucune erreur : les cyberprédateurs/cyberprédatrices sont omniprésent(e)s sur le Net et sont très dangereux/dangereuses.

D'autres cyberprédateurs/cyberprédatrices sont plus subtil(e)s. Ils/elles ne cherchent pas la satisfaction sexuelle, mais veulent profiter de vous pour leurs propres intérêts personnels - quelquefois émotifs, financiers ou même dans le but d'immigrer. Votre meilleur moyen de défense pour ne pas tomber dans leur piège est de connaître les caractéristiques d'un prédateur/prédatrice et d'utiliser votre intelligence pour les éviter.

Ce qu'il faut faire une fois ciblé(e) par un cyberprédateur/une cyberprédatrice :

- **Ne gardez pas cela secret :**

Si vous recevez un ou plusieurs messages qui vous déstabilisent ou vous harcèlent, les chances sont que vous êtes victime de cyberintimidation. Informez alors quelqu'un(e) en qui vous avez confiance, tel(le) qu'un(e) parent, membre de la famille, formateur/formatrice collègue ou

conseiller/conseillère. En parler à un(e) ami(e) peut aider, mais n'hésitez pas à en parler à quelqu'un(e) qui a peut-être plus d'expérience dans la gestion de ce type d'harcèlement. Il y a aussi des organisations comme l'Association des Juristes Sénégalaise (AJS) qui peuvent vous donner des conseils de façon anonyme. Si le ou les messages que vous avez reçus sont menaçants ou harcelants, vous devriez en informer votre police locale.

- **Traiter votre email comme un numéro de téléphone :**

Donnez votre adresse email aux gens que vous connaissez déjà et en qui vous avez confiance et soyez prudent(e) quand vous publiez votre email sur un site web, un site de clavardage en ligne (site de discussion) ou un service de messagerie instantanée. De plus, ne distribuez pas les emails de vos ami(e)s sans leur autorisation. Avoir le contrôle sur vos conversations en ligne est la meilleure mesure de sécurité. C'est à vous de décider avec qui vous discutez ; il ne faut donc pas laisser les autres vous forcer à discuter avec eux en vous donnant des noms inamicaux ou autres. Bien que vous puissiez changer votre adresse email si vous recevez trop d'emails indésirables, vous avez déjà pu être exposé(e)à des emails offensants ou inquiétants.

- **Apprenez comment bloquer des expéditeurs/expéditrices :**

Vérifiez les options ou préférences dans votre compte email ou service de messagerie instantanée afin de connaitre les moyens de bloquer des utilisateurs/utilisatrices qui vous contactent. Parfois, vous devez ajouter l'expéditeur/expéditrice sur la liste des utilisateurs/utilisatrices bloqué(e)s et d'autres fois, vous pouvez cliquer sur le nom et sélectionner l'option « bloquer ».

- **Soyez prudent(e)lorsque vous ~~ne~~ rencontrez en personne un(e) ami(e) que vous vous êtes fait(e) en ligne :**

Il n'y a pas de règles absolues dans l'espace virtuel. Quelques sites vous conseilleront de ne jamais rencontrer en personne ceux et celles que vous avez rencontré en ligne, mais ce niveau de précaution est irréaliste et restrictif. Le Web abrite des communautés où plusieurs bonnes personnes jouent et travaillent. Si vous faites des rencontres en ligne, vous n'avez pas à présumer qu'ils/elles veulent quelque chose de vous autre que l'amitié. Bien sûr, vous devez être prudent(e) ; quand vous rencontrez, en personne un(e) nouvel(le) ami(e) que vous vous êtes fait en ligne, amenez une personne de confiance ou rencontrez-le/ la dans un milieu public où vous avez le contrôle de la situation à tous moments.

8.7: Est-ce que *vous* vous comportez comme un cyberintimidateur/une cyberintimidatrice[12] ?

Certains cyberintimidateurs/certaines cyberintimidatrices ne savent pas que leurs actions sont intimidatrices, parce qu'en personne, ils/elles ne sont pas des oppresseurs et paraissent même timides. Certain(e)s peuvent même déjà avoir été victimes d'intimidation et utilisent le Net pour se venger. Il faut être conscient(e) de nos propres comportements pouvant être

[12]Adapté de Taking it Global's website,25Octobre 2015:

https://www.tigweb.org/themes/onlinesafety/cyber_bullying_and_predators.html, 25Octobre 2015

considérés comme de la cyberintimidation. Examinez la liste ci-dessous pour voir si vous avez déjà intimidé quelqu'un(e). Cochez les points qui s'appliquent à vous :

- ❑ J'ai continué à contacter quelqu'un(e), même après qu'il/elle m'ait ignoré(e) à maintes reprises ;
- ❑ J'ai envoyé des emails sous l'effet de la colère en mentionnant des noms et en utilisant un langage agressif ;
- ❑ J'ai essayé de contacter quelqu'un(e) même après qu'il/elle m'ait bloqué(e) ;
- ❑ J'ai envoyé un email menaçant ;
- ❑ J'ai partagé des histoires gênantes et des secrets à propos des autres à travers des emails ou sites web ;
- ❑ J'ai parfois réagi d'une manière agressive en ligne parce que c'est difficile de ne le faire en personne.

Si vous vous êtes comporté(e)de l'une ou l'autre de ces façons, c'est le moment de changer votre « netiquette » (étiquette sur le Net). Vous n'êtes peut-être pas un cyberintimidateur/une cyberintimidatrice à part entière, mais vous avez sans aucun doute affiché un comportement hostile en ligne et cela vous rend coupable de harcèlement. N'utilisez pas le Net comme moyen d'exprimer votre frustration ou vos ressentiments. Cherchez de vraies solutions à vos sentiments et évitez d'attaquer les autres - même s'ils/elles sont la source de votre frustration. Souvenez-vous : n'envoyez pas d'emails quand vous êtes fâché(e). Attendez jusqu'à ce que vous vous calmiez pour contacter quelqu'un(e).

8.8: Conseils généraux pour devenir un(e) cybercitoyen(ne)[13] :

Qu'est-ce que ça veut dire être un(e) cybercitoyen(ne) ? Comment est-ce que nous devrions agir dans ce monde sans limite ? Comment pouvons-nous assurer notre sécurité et continuer à profiter de tout ce que le Web a à offrir ? Pour être un(e) cybercitoyen(ne) efficace et productif/productive, il faut :

- ✓ Protéger sa propriété intellectuelle : La propriété intellectuelle fait référence à toutes vos idées, expressions, créations, etc. qui sont originales. Ce peut être un écrit tel qu'un article ou un livre, une photo, une vidéo, une chanson, etc. ;
- ✓ Signaler toute personne qui intimide et ne pas harceler les autres ;
- ✓ Protéger son identité ;
- ✓ Ne pas prétendre être quelqu'un d'autre pour profiter des autres ;
- ✓ Utiliser ses connaissances du Net dans tout ce que l'on fait ;

[13]Taking it Global le25 octobre 2015: https://www.tigweb.org/themes/onlinesafety/cyber_citizenship.html

- ✓ Ne pas avoir peur de poser des questions ;
- ✓ Faire des recherches sur les organisations qui demandent nos informations personnelles ;
- ✓ Être gentil(le) et respectueux/respectueuse autant qu'on le peut ;
- ✓ Et ***toujours*** être conscient(e) de sa responsabilité relativement à ce que l'on dit et fait en ligne !

Séance 3: Chercher des ressources en ligne

🗝 Sujets clés 🗝

- Information : est-ce qu'elle est vraie ou fausse ?
- Stratégies pour déterminer quelles sont les informations les plus fiables ;
- Comment chercher des ressources en ligne.

8.9: Comment utiliser les modificateurs de recherche ?

Le « top 5 » des modificateurs de recherche pour faire des recherches avancées sur le Net par le biais de Google[14]:

1. "**Requête**"… guillemets, ou "requête" instruira Google de chercher seulement l'information relative à la question, aussi connu comme recherche d'équivalence exacte ;
2. **Requête**… le modificateur de soustraction enlèvera toute question que vous ne voulez pas dans les résultats de recherche ;
3. **Requête AND requête**… utiliser « AND » dans la recherche permettra de vous assurer que les deux requêtes paraissent dans tous les résultats ;
4. **Requête OU requête**… permet de chercher de multiples termes ;
5. **Site : exemple.com… site : exemple.com va raffiner la recherche de Google à un seul site web.**

[14] http://searchengineland.com/top-10-search-modifiers-why-they-matter-what-they-are-how-to-use-them-173343, 28Octobre 2015.

Autoévaluation
Module 8 : Culture numérique

Il n'y a ni bonnes ni mauvaises façons de répondre à cette activité d'autoévaluation. Nous voulons juste recueillir vos manières de penser et de faire pour nous aider à mieux dérouler ce qui va suivre. Ceci servira également à votre usage personnel lors de ce cours. Le professeur/la professeure va lire une compétence énumérée dans la colonne de gauche.
Lisez les choix dans la partie supérieure. En pensant à vous-même, dites quel point représente le mieux votre situation en cochant la case correspondante dans chaque colonne.

Mon expérience **Connaissances, compétences et capacités**	**(1)** **Je n'ai aucune connaissance à ce sujet**	**(2)** **J'ai peu de connaissances à ce sujet**	**(3)** **J'ai quelques connaissances à ce sujet pour parfois le faire correctement**	**(4)** **J'ai beaucoup de connaissances à ce sujet et je peux le faire régulièrement**	**(5)** **J'ai beaucoup de connaissances à ce sujet et je peux le faire correctement et de façon consistante**
Créer une présence en ligne par email et par les plates-formes de réseaux sociaux telles que Facebook, Youtube, etc.,					
Déterminer les moyens par lesquels je peux présenter en ligne mes compétences, aptitudes, expériences et intérêts					
Consulter et analyser la présence en ligne de certaines personnes pour identifier les éléments de succès et stratégies de présentation en ligne					

Mon expérience Connaissances, compétences et capacités	(1) Je n'ai aucune connaissance à ce sujet	(2) J'ai peu de connaissances à ce sujet	(3) J'ai quelques connaissances à ce sujet pour parfois le faire correctement	(4) J'ai beaucoup de connaissances à ce sujet et je peux le faire régulièrement	(5) J'ai beaucoup de connaissances à ce sujet et je peux le faire correctement et de façon consistante
Identifier comment utiliser une présence en ligne pour trouver de l'emploi ou développer ma propre entreprise					
Faire usage des pratiques de sécurité lorsque je suis en ligne pour me protéger contre les pirates informatiques, les escrocs, etc.					
Reconnaitre la cyberintimidation, y compris l'humiliation et l'agression					
Prendre une position proactive contre la cyberintimidation					
Utiliser la pensée critique pour analyser des ressources en ligne (qui envoie, pourquoi, source de l'information, etc.)					
Chercher efficacement des ressources en ligne					
Utiliser des ressources en ligne pour trouver du travail					