Fiche de formationE-Seniors

|  |  |
| --- | --- |
| **Titre** | **Thème : Information et communication via les réseaux sociaux**  **Unité 3. Menaces et défis sur les réseaux sociaux : FAIRE et NE PAS FAIRE** |
| **Zone d'entraînement** | *Veuillez sélectionner une ou plusieurs des options suivantes :*   |  |  | | --- | --- | | Sécurité en ligne |  | | Littérature culturelle et médiatique | *X* | | Transactions économiques |  | | Protection des données personnelles |  | | Identité numérique et e-réputation |  | |
| **Mots clés (balise meta)** | **Réseaux sociaux, communication, sécurité** |
| **Fourni par** | **E-Seniors** |
| **Langue** | **Français** |
| **Objectifs / buts / résultats d'apprentissage** | |
| Ce module vise à développer les connaissances et les compétences des utilisateurs sur la façon d'utiliser les réseaux sociaux pour la communication et la promotion de la culture et de la créativité. Les utilisateurs seniors se familiariseront avec les outils de réseaux sociaux, des ressources culturelles sur les médias sociaux qui leur permettent de naviguer facilement et de découvrir des opportunités culturelles et de communication. | |
| **La description** | |
| La formation est aménagée en 3 niveaux : chaque module est divisé en unités et contenus. Les titres des unités donnent une idée plus détaillée du contenu du module. Ce module spécifique est construit comme suit :  **Thème : Information et communication via les réseaux sociaux**  **Module 3. Menaces et défis sur les réseaux sociaux : FAIRE et NE PAS FAIRE**  **Unité 3.1 :**Menaces et défis  **Unité 3.2 :**10 bonnes pratiques à adopter pour la sécurité sur les réseaux sociaux. | |
| **Contenu organisé en 3 niveaux** | |
| **Module 3 : Menaces et défis sur les réseaux sociaux : choses à faire et à ne pas faire**  Il existe de nombreuses menaces et défis liés à la navigation sur Internet, à la fois sur l'ordinateur et le smartphone. Les réseaux sociaux ne font pas exception. L'utilisation des réseaux sociaux comporte plusieurs risques. Cependant, si des précautions sont prises, il n'est pas difficile de surfer avec un minimum de risques.  **Unité 3.1 :**Menaces et défis   * **Hameçonnage:** L'hameçonnage est un procédé dans lequel un attaquant envoie un message frauduleux conçu pour tromper une victime humaine. Ces messages sont conçus pour vous inciter à révéler des informations personnelles en prétendant provenir d'une source fiable. Les messages peuvent provenir de personnes prétendant être un de vos amis ou une entreprise connue. Ne partagez jamais d'informations confidentielles et ne cliquez jamais sur un lien Web suspect. * **Piratage psychologique :**Le piratage psychologique consiste à obtenir des informations confidentielles d'une personne par ruse. Le fraudeur peut entamer une conversation sur des choses qu'il a lues sur votre profil, comme votre lieu de travail, etc. Il essaie ensuite de vous faire révéler des informations personnelles.informations similaires à du phishing. * **Logiciels malveillants :**Les logiciels malveillants sont des logiciels malveillants conçus pour infiltrer les appareils. Il circule sur les réseaux sociaux sous forme de liens avec des titres accrocheurs. Une fois le logiciel malveillant infiltré, il peut envoyer des messages aux contacts, accéder à des informations personnelles ou endommager l'appareil. La prudence s'impose lorsqu'on est tenté de cliquer sur un lien provenant d'une source inconnue. * **Discours de haine :**Le discours de haine est courant sur les réseaux sociaux car ses auteurs peuvent rester anonymes. Il peut arriver que vous receviez des propos haineux, parfois sans aucun réseau, il est donc important de vous en détacher et de ne pas hésiter à les signaler comme contenu indésirable et malveillant. * **Harcèlement sur internet:**est l'intimidation qui se produit sur des appareils numériques comme les téléphones cellulaires, les ordinateurs et les tablettes. La cyberintimidation peut se produire par SMS, SMS et applications, ou en ligne sur les réseaux sociaux, les forums ou les jeux où les gens peuvent voir, participer ou partager du contenu. La cyberintimidation comprend l'envoi, la publication ou le partage de contenu négatif, nuisible, faux ou méchant à propos de quelqu'un d'autre. Cela peut inclure le partage d'informations personnelles ou privées sur quelqu'un d'autre causant de l'embarras ou de l'humiliation. Certains actes de cyberintimidation franchissent la frontière avec un comportement illégal ou criminel. * **L'âgisme en ligne**: L'âgisme fait référence aux stéréotypes (comment nous pensons), aux préjugés (comment nous nous sentons) et à la discrimination (comment nous agissons) envers les autres ou envers soi-même en fonction de l'âge. L'âgisme touche tout le monde. Dès l'âge de 4 ans, les enfants prennent conscience des stéréotypes d'âge de leur culture. À partir de cet âge, ils intériorisent et utilisent ces stéréotypes pour orienter leurs sentiments et leur comportement envers les personnes d'âges différents. Ils s'appuient également sur les stéréotypes liés à l'âge de la culture pour se percevoir et se comprendre, ce qui peut entraîner un âgisme auto-dirigé à tout âge. L'âgisme recoupe et exacerbe d'autres formes de désavantages, notamment ceux liés au sexe, à la race et au handicap. * **À quoi faire attention pour éviter les escroqueries sur Facebook :**   + Les personnes que vous ne connaissez pas personnellement qui vous demandent de l'argent ou vos coordonnées bancaires.   + Les pages non vérifiées qui prétendent représenter une grande organisation ou une personnalité publique.   + Les personnes qui vous demandent de poursuivre votre conversation en dehors de Facebook, dans un lieu moins public ou moins sécurisé, comme une adresse e-mail distincte.   + Les personnes qui vous demandent de leur transmettre vos coordonnées bancaires afin de recevoir une récompense.   + Toute personne prétendant être un ami ou un parent en détresse.   + Les gens qui mentent sur leur lieu de résidence.   + Les messages ou publications contenant des fautes d'orthographe et des erreurs grammaticales.   + Les personnes ou comptes qui vous redirigent vers une Page pour réclamer un prix   **Unité 3.2 : 10 bonnes pratiques à adopter pour la sécurité sur les réseaux sociaux :**  1- Protégez l'accès à vos comptes : Utilisez des mots de passe forts et différents d'un compte à l'autre.Les applications de gestion de mots de passe peuvent vous aider à enregistrer facilement vos mots de passe. Par exemple https://keepassxc.org/  2- Vérifiez vos paramètres de confidentialité : Par défaut, les paramètres de confidentialité sont souvent ouverts (sur les informations personnelles telles que le nom, le numéro de téléphone, l'adresse e-mail). Ces données peuvent être accessibles à tous les abonnés du réseau social. Il est possible de limiter cette visibilité en ajustant la configuration du compte pour garder le contrôle de ce que voient les autres utilisateurs.  3- Contrôlez vos messages : vos messages peuvent devenir incontrôlables et être republiés ou interprétés plus que vous ne le vouliez. Ne publiez pas d'informations personnelles ou sensibles.  4- Faites attention à qui vous parlez vos amis peuvent partager du contenu malveillant sans le savoir, ou peuvent avoir été piratés eux-mêmes. N'envoyez jamais d'argent sans vérifier l'identité de la personne, n'envoyez pas de vidéos privées, méfiez-vous des concours, des gains inattendus ou des « bonnes affaires » qui pourraient cacher des arnaques.  5- Contrôlez les applications tierces : Certaines applications proposent d'interagir avec l'un de vos comptes de réseaux sociaux. Ils nécessitent des autorisations qui doivent être examinées avec précaution car certains d'entre eux pourraient alors avoir accès à vos données. Veillez à ne pas installer d'applications que vous soupçonnez d'être malveillantes.  6- Evitez les ordinateurs et les réseaux publics : Utiliser un ordinateur en libre accès ou un Wi-Fi public est risqué car ils peuvent être compromis ou sous le contrôle de cybercriminels. Évitez de saisir des informations sensibles ou de les utiliser si possible.  7- Vérifiez régulièrement les connexions à votre compte : La plupart des réseaux sociaux vous permettent de voir les connexions ou les sessions actives du compte. Vérifiez régulièrement ces informations pour vous assurer qu'aucun autre appareil n'est connecté à l'un de vos comptes. Si c'est le cas, déconnectez-le et changez votre mot de passe.  8- Soyez conscient des fausses informations: Certaines informations publiées peuvent être fausses, délibérément ou non. Avant d'envisager ou de relayer une information, vérifiez son authenticité.  9- Vérifiez vos identifications avec vos comptes : Certains sites proposent de vous inscrire avec votre compte de réseau social. Cela évite d'avoir à créer un mot de passe, par exemple, mais peut fournir des données personnelles au site ou permettre à un cybercriminel qui a piraté votre réseau social d'accéder également à votre compte sur ce site.  10- Supprimez votre compte si vous ne l'utilisez plus : Pour éviter tous les risques décrits ci-dessus, pour vous assurer que votre compte n'est pas utilisé à votre insu, supprimez votre compte lorsque vous n'en avez plus besoin. | |
| **Contenu en puces** | |
| * Les menaces et les défis les plus fréquents liés à l'utilisation des médias sociaux consistent à se défendre contre le phishing, les logiciels malveillants, les discours de haine, etc. ; * Vous pouvez éviter les menaces et les risques des médias sociaux en suivant les recommandations et conseils stipulés dans ce module de formation | |
| **5 entrées de glossaire** | |
| **Sécurité des réseaux sociaux :**La sécurité des médias sociaux fait référence à toutes les mesures que l'utilisateur doit prendre pour éviter les risques, les escroqueries et les attaques sur son compte personnel.  **Discours de haine :**Les discours de haine sont des mots prononcés qui sont offensants, insultants et/ou menaçants pour un individu ou un groupe en fonction d'un attribut particulier de cette personne ou des personnes ciblées.  **Piratage psychologique :**Le piratage psychologique consiste à obtenir des informations confidentielles d'une personne par ruse.  **Harcèlement sur internet:**est l'intimidation qui a lieu sur des appareils numériques comme les téléphones cellulaires, les ordinateurs et les tablettes  **L'âgisme en ligne**: L'âgisme fait référence aux stéréotypes (comment nous pensons), aux préjugés (comment nous nous sentons) et à la discrimination (comment nous agissons) envers les autres ou envers soi-même en fonction de l'âge. L'âgisme touche tout le monde. | |
| **Bibliographie et autres références** | |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)  [**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) | |
| **Cinq questions d'auto-évaluation à choix multiples** | **1) Il est sûr d'utiliser des ordinateurs publics**   1. **Vrai** 2. **Faux**   **Correct : B**  **2) Qu'est-ce qu'un logiciel malveillant ?**   1. **Logiciels malveillants conçus pour infiltrer les appareils** 2. **Vol d'identité** 3. **Discours de haine**   **Correct : A**  **3) Qu'est-ce que le discours de haine ?**   1. **Les discours de haine sont des mots prononcés qui sont offensants, insultants et/ou menaçants pour un individu ou un groupe en fonction d'un attribut particulier de cette personne ou des personnes ciblées.** 2. **Le discours de haine est le processus qui consiste à obtenir des informations confidentielles d'une personne par ruse.** 3. **Le discours de haine est une information malveillante conçue pour infiltrer les appareils et attaquer les humains.**   **Correct : A**  **4) Sécurité des réseaux sociaux :**   1. **Désigne toutes les mesures que les entreprises utilisent pour lutter contre la fraude en ligne.** 2. **Désigne toutes les mesures que l'utilisateur doit prendre pour éviter les risques, les arnaques et les attaques sur son compte personnel.** 3. **Référez-vous aux outils des médias sociaux conçus pour les utilisateurs.**   **Correct : B**  **5) Que faire si vous tombez sur le discours de haine en ligne ?**   1. **Essayez d'éviter les attaquants** 2. **Essayez de signaler les agresseurs** 3. **Toutes les réponses sont bonnes**   **Correct : C** |
| **Matériel connexe** | **Comment identifier et éviter les escroqueries courantes sur les réseaux sociaux :<https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/>**  **Comment éviter la fraude sur les réseaux sociaux :[https://www.bnc.ca/personnel/conseils/securite/fraude-medias-sociaux-arnaques.html](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)**  **Cyberintimidation et discours de haine :<https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf>** |
| **PPT associés** |  |
| **Lien de référence** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **Vidéo au format YouTube (le cas échéant)** | **Qu'est-ce que les médias sociaux ? En anglais simplifié :**  [**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)  **Amazing Mind Reader révèle son "don":**[**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |