Fiche de formation CDI

|  |  |
| --- | --- |
| **Titre** | Comment identifier les informations manquantes et les fausses nouvelles en ligne dans un contexte culturel pertinent ? |
| **Zone d'entraînement** | *Veuillez sélectionner une ou plusieurs des options suivantes :*

|  |  |
| --- | --- |
| Sécurité en ligne | X |
| Littérature culturelle et médiatique |  |
| Transactions économiques |  |
| Protection des données personnelles |  |
| Identité numérique et e-réputation |  |

 |
| **Mots clés (balise meta)** | Sécurité en ligne, contexte culturel, fausses nouvelles, informations manquantes |
| **Fourni par** | Institut de développement communautaire, CDI |
| **Langue** | Français |
| **Objectifs / buts / résultats d'apprentissage** |
| À la fin de ce module, vous acquerrez des connaissances en matière de reconnaissance des fausses nouvelles et des informations manquantes ainsi que de la sécurité en ligne dans un contexte culturel.Le module se compose de quatre unités fournissant des informations relatives au sujet dans différentes sections. Différentes activités et remerciements sont étayés par des exemples pour une meilleure compréhension du matériel, des photos explicatives et des liens utiles pour approfondir vos connaissances sur le sujet.Les utilisateurs auront la possibilité d'être initiés à la sécurité en ligne dans un contexte culturel ainsi qu'à la sécurité en ligne. Les menaces de sécurité en ligne possibles seront présentées à travers des explications sur les différents types de menaces comme les logiciels malveillants, le phishing, les attaques par mot de passe, etc.Les utilisateurs pourront :● Comprendre la signification de la sécurité et de la sûreté en ligne ● Faites la différence entre les fausses nouvelles, la désinformation et les informations manquantes ● Utiliser différents conseils concernant la sécurité en ligne dans un contexte culturel  |
| **La description** |
| Les technologies numériques ont révolutionné tous les aspects de nos vies. Ils ont eu un impact sur les chaînes de valeur de toutes les industries culturelles et créatives non seulement en ce qui concerne le processus créatif et son exécution, mais aussi en ce qui concerne la fabrication d'une œuvre ou d'un produit d'art et sa promotion, sa distribution, sa commercialisation et sa vente.Cette unité d'apprentissage apprendra aux digitals tardifs à détecter les escroqueries potentielles qu'ils pourraient rencontrer sur le web lors de l'utilisation ou de la recherche de ressources culturelles. Cette unité fournira des exemples spécifiques d'escroqueries courantes liées aux ressources culturelles, telles que les fausses ventes de billets, les tentatives de phishing après une commande en ligne, etc. Elle donnera également les points clés pour identifier les ressources culturelles sécurisées en ligne.À l'ère de la technologie, les fausses nouvelles et les informations manquantes font partie de la circulation quotidienne et de l'information en ligne. Les utilisateurs seront initiés à la signification des fausses nouvelles et des informations manquantes, comment reconnaître les fausses nouvelles et l'importance de différencier les fausses nouvelles des informations manquantes.Favoriser la capacité à reconnaître et à se protéger contre les informations manquantes et les fausses nouvelles est l'unité fournissant des informations et du contenu concernant la capacité des utilisateurs à se protéger en ligne. Des trucs et astuces sont fournis avec des exemples et des photos utiles. |

|  |
| --- |
| **Contenu organisé en 3 niveaux** |
| 1. **INTRODUCTION**
2. **CONTENU**

**Unité 1 : Qu'est-ce que la sécurité en ligne ?**1.1 Sécurité en ligne et sécurité en ligne, c'est-à-dire1.2 Sécurité en ligne dans les contenus culturels**Unité 2 : Les plus grandes menaces pour votre sécurité en ligne**2.1 Types de menaces de sécurité en ligne* Logiciels malveillants
* L'homme du milieu MITM
* Hameçonnage
* Attaques de mot de passe

**Unité 3 : Identifier les informations manquantes, la mésinformation, la désinformation et les fausses nouvelles dans un contexte culturel**3.1 D'où viennent les fausses nouvelles ?3.2 Comment reconnaître les fausses nouvelles, la mésinformation, la désinformation et les informations manquantes dans le contexte culturel**Unité 4 : Se protéger des menaces de sécurité en ligne**4.1 Protégez-vous lorsque vous êtes en ligne4.2 Conseils pour la sécurité en ligne dans un contexte culturel1. **CONCLUSION**

**Module : Comment identifier les informations manquantes et les fausses nouvelles en ligne dans un contexte culturel pertinent**1. **INTRODUCTION**

Les technologies numériques ont révolutionné tous les aspects de nos vies. Ils ont eu un impact sur les chaînes de valeur de toutes les industries culturelles et créatives non seulement en ce qui concerne le processus créatif et son exécution, mais aussi en ce qui concerne la fabrication d'une œuvre ou d'un produit d'art et sa promotion, sa distribution, sa commercialisation et sa vente. Alors que le virage numérique se poursuit, de plus en plus d'artistes, de cinéastes, de producteurs, de musiciens, etc. distribuent leurs produits par voie numérique. À la fin de ce module, vous acquerrez des connaissances et une reconnaissance des fausses informations nouvelles et manquantes ainsi que de la sécurité en ligne dans un contexte culturel.Dans un monde où une attaque de pirate informatique a lieu environ toutes les 39 secondes, la sécurité en ligne ne peut plus être prise à la légère. Sinon, toutes vos données personnelles pourraient être en danger.Mais qu'est-ce que la sécurité en ligne, pour être exact ? Quels types de menaces existent sur le Web et que pouvez-vous faire pour vous en protéger ? Une menace à la sécurité en ligne fait référence à toute attaque malveillante potentielle qui cherche à accéder illégalement à des données, à perturber des opérations numériques ou à endommager des informations. Maintenant, plus que jamais, le contenu culturel est largement accessible, il est également ouvert aux menaces en ligne, la diffusion d'informations manquantes, la désinformation, la désinformation et les fausses nouvelles pourraient nuire à l'expérience d'une personne tout en appréciant et en informant sur un spectacle ou un événement culturel.**Unité 1 : Qu'est-ce que la sécurité en ligne ?****Section 1.1 Expliquer la sécurité en ligne et la sécurité en ligne**La sécurité Internet consiste en une gamme de tactiques de sécurité pour protéger les activités et les transactions effectuées en ligne sur Internet. Ces tactiques sont destinées à protéger les utilisateurs contre les menaces telles que le piratage des systèmes informatiques, des adresses e-mail ou des sites Web. La sécurité Internet est un aspect spécifique de concepts plus larges tels que la cybersécurité et la sécurité informatique, qui se concentre sur les menaces et les vulnérabilités spécifiques de l'accès en ligne et de l'utilisation d'Internet.**La sécurité en ligne** protège les personnes utilisant Internet contre les dommages par la sensibilisation, l'éducation, l'information et la technologie. La sécurité en ligne est consciente de la nature des menaces possibles que vous pourriez rencontrer lors de vos activités sur Internet, il peut s'agir de menaces à la sécurité, de la protection et de la gestion de vos données personnelles en ligne et de la prévention des contenus préjudiciables ou illégaux.**Section 1.2 Sécurité en ligne des contenus culturels**Les technologies numériques ont révolutionné tous les aspects de nos vies, et la culture ne fait pas exception. Ils ont eu un impact sur les chaînes de valeur de toutes les industries culturelles et créatives non seulement en ce qui concerne le processus de création et son exécution, mais également en ce qui concerne la fabrication d'une œuvre ou d'un produit d'art et sa promotion, sa distribution, sa commercialisation et sa vente. Certains processus de production sont uniquement numériques et la technologie a un énorme potentiel pour rendre la culture accessible à tous, en démocratisant à la fois la consommation et la participation à la création culturelle.Dans le même temps, les institutions culturelles telles que les musées, les archives, les bibliothèques et les diffuseurs de films, de télévision et de musique ont numérisé leurs collections dans le but de les préserver et de les rendre plus largement disponibles. Parfois, la numérisation est une étape nécessaire, comme dans le cas des films analogiques, qui ne peuvent plus être projetés dans leur forme originale, car les cinémas sont équipés uniquement de technologie numérique.Une multitude de contenus culturels numériques sont disponibles en ligne gratuitement, moyennant des frais ou illégalement. Une telle disponibilité et abondance de contenu culturel et les diverses façons de le consulter en ligne apportent de nouveaux défis et opportunités pour perturber la sécurité en ligne d'une personne par divers moyens. Il est donc important, en cette ère numérique, d'être informé et de connaître les menaces qui pèsent sur votre sécurité en ligne et de savoir comment vous protéger lorsque vous accédez à du contenu culturel en ligne.**Unité 2 : Les plus grandes menaces pour votre sécurité en ligne****Section 2.1 Types de menaces de sécurité en ligne**Une menace à la sécurité en ligne fait référence à toute attaque malveillante potentielle qui cherche à accéder illégalement à des données, à perturber des opérations numériques ou à endommager des informations.Il existe des dizaines de menaces de sécurité en ligne sur Internet, nous avons donc décidé de nous concentrer sur les plus dangereuses et les plus courantes.**Logiciels malveillants :**Les logiciels malveillants sont des logiciels malveillants tels que les logiciels espions, les rançongiciels, les virus et les vers. Les logiciels malveillants sont activés lorsqu'un utilisateur clique sur un lien ou une pièce jointe malveillants, ce qui conduit à l'installation de logiciels dangereux que les logiciels malveillants, une fois activés, peuvent :● Bloquer l'accès aux composants clés du réseau (ransomware) ●Installer des logiciels nuisibles supplémentaires ● Obtenir secrètement des informations en transmettant des données depuis le disque dur (logiciel espion) ● Perturber des pièces individuelles, rendant le système inutilisable **L'homme du milieu, MITM :**Une menace de l'homme du milieu (MITM) se produit lorsque des acteurs malveillants s'insèrent dans une transaction à deux parties. Après avoir interrompu la transaction, ils peuvent filtrer et voler des données. La menace MITM se réalise souvent lorsqu'un visiteur utilise un réseau Wi-Fi public non sécurisé. Les acteurs malveillants s'insèrent entre le visiteur et le réseau, puis utilisent les logiciels malveillants mentionnés précédemment pour installer des logiciels et utiliser les données de manière malveillante.**Hameçonnage:**Les attaques de phishing utilisent de fausses communications, telles qu'un e-mail, pour inciter le destinataire à l'ouvrir et à exécuter les instructions qu'il contient, telles que fournir un numéro de carte de crédit. L'objectif est de voler des données sensibles telles que les informations de carte de crédit et de connexion ou d'installer des logiciels malveillants sur la machine de la victime.**Attaques par mot de passe :**Avec le bon mot de passe, un acteur malveillant a accès à une mine d'informations. L'ingénierie sociale est un type d'attaque par mot de passe défini comme "une stratégie qui repose fortement sur l'interaction humaine et implique souvent d'inciter les gens à enfreindre les pratiques de sécurité standard".D'autres types d'attaques par mot de passe incluent l'accès à une base de données de mots de passe ou la supposition pure et simple.**Unité 3 : Identifier les informations manquantes, la mésinformation, la désinformation et les fausses nouvelles dans un contexte culturel**Maintenant, plus que jamais, le contenu culturel est largement accessible et ouvert aux menaces en ligne, la diffusion d'informations manquantes, la désinformation, la désinformation et les fausses nouvelles pourraient nuire à l'expérience d'une personne tout en appréciant et en s'informant sur un événement ou un espace culturel.**Section 3.1 Qu'entend-on par fausses nouvelles, mésinformation et désinformation ?****Les fausses nouvelles (Fake news)** sont des informations délibérément conçues, sensationnelles, chargées d'émotions, trompeuses ou totalement fabriquées.Il existe deux types de fake news :1. Des histoires qui ne sont pas vraies. Ce sont des histoires entièrement inventées conçues pour inciter les gens à croire quelque chose de faux, à acheter un certain produit ou à visiter un certain site Web.2. Des histoires qui ont une part de vérité, mais qui ne sont pas exactes à 100 %. Encore une fois, cela peut être délibéré, pour convaincre les lecteurs d'un certain point de vue, ou cela peut être le résultat d'une erreur innocente.Le terme désinformation fait référence à des informations fausses ou inexactes et qui sont souvent largement diffusées auprès d'autres personnes, quelle que soit l'intention de tromper.Alors que la désinformation est une fausse information qui est créée et diffusée indépendamment d'une intention de nuire ou de tromper, la désinformation est un type de désinformation qui est créée pour être délibérément trompeuse. Les deux formulaires peuvent être largement partagés, indépendamment desi le partageur sait que l'information est erronée.Les plateformes de médias sociaux permettent à presque tout le monde de publier ses pensées ou de partager des histoires avec le monde. Le problème est que la plupart des gens ne vérifient pas la source du contenu qu'ils consultent en ligne avant de le partager, ce qui peut entraîner la diffusion rapide de fausses nouvelles. Dans le même temps, il est devenu plus difficile d'identifier la source originale des reportages, ce qui peut compliquer l'évaluation de leur exactitude.**Section 3.2 Comment reconnaître les fausses nouvelles, la désinformation, la désinformation et les informations manquantes dans le contexte culturel**Comment repérer les fausses nouvelles, la désinformation, la désinformation et les informations manquantes, posez-vous les questions suivantes et procédez comme suit :● **Qui l'a écrit?** Vérifiez le nom de l'auteur. Le nom est-il disponible ou manque-t-il ? La plupart des auteurs qui consacrent du temps à un article bien documenté y verront probablement leur nom.● **Quelles sont leurs qualifications ?**Si le nom de l'auteur est répertorié, découvrez qui est la personne et quelles sont ses références.● **Consultez la section "À propos de nous"**. En haut ou en bas du site Web, il devrait y avoir une section intitulée "À propos de nous". Cette section décrit l'objectif du site Web.● **L'article vous informe-t-il de tous les aspects du sujet ?**Les articles de presse doivent vous fournir des faits de différents points de vue.● **Le contenu correspond-il au titre de l'article ?**Un titre devrait vous donner une idée du sujet de l'article dans son ensemble, mais il peut également être utilisé pour vous persuader de croire quelque chose avant de lire l'article.● **Quand cet article a-t-il été publié ?**Les articles plus anciens peuvent ne pas contenir de faits à jour et peuvent avoir des liens brisés.● **L'article a-t-il été réutilisé ou mis à jour ?**Le contenu réutilisé ou mis à jour a tendance à avoir une clause de non-responsabilité au début ou à la fin de l'article.● Quelle est l'importance de la date ? La date vous donne une indication de la date de publication de l'article. ● **Cette adresse Web (URL) semble-t-elle correcte ?**Si vous tapez la mauvaise adresse Web, vous serez dirigé vers une page Web que vous n'aviez pas l'intention de visiter. Cela peut vous conduire à une page avec les menaces de sécurité en ligne mentionnées ci-dessus.● **Est-ce que j'ai trouvé ça sur les réseaux sociaux ? Les plateformes de médias sociaux ne sont pas des organes de presse. Ce sont des plateformes permettant aux personnes de créer et/ou de partager du contenu.**● **Ai-je trouvé cela sur un blog/site Web ?**Les blogs contiennent du contenu écrit de manière informelle et géré par un individu ou un petit groupe.**Unité 4 : Se protéger des menaces de sécurité en ligne****Section 4.1 Protégez-vous lorsque vous êtes en ligne**Voici certaines choses que vous pouvez améliorer pour vous protéger lorsque vous êtes en ligne :1. **N'utilisez pas de réseaux Wi-Fi non sécurisés**

Il est préférable d'éviter tout réseau Wi-Fi qui ne vous demande pas de mot de passe et utilisez simplement votre propre forfait de données mobiles à la place.**2. Utilisez un logiciel antivirus puissant**Un logiciel antivirus est votre meilleur pari pour protéger votre appareil contre les infections par des logiciels malveillants dont nous avons parlé. Ne laissez pas le nom vous confondre - un programme antivirus lutte contre les virus, mais il cible principalement les logiciels malveillants (un virus étant un type de logiciel malveillant). Assurez-vous de maintenir le programme à jour et d'effectuer des analyses fréquentes, en particulier après avoir téléchargé de nouveaux fichiers. Il est préférable de ne pas les ouvrir sans les scanner au préalable, en fait.**3. Utilisez toujours un VPN en ligne**Un VPN (Virtual Private Network) est un service en ligne que vous pouvez utiliser pour masquer votre véritable adresse IP et crypter vos communications en ligne. C'est l'un des meilleurs moyens d'améliorer votre sécurité en ligne et de masquer vos empreintes numériques. Tant que les méthodes de cryptage appropriées sont utilisées, personne ne pourra surveiller votre trafic en ligne pour voir ce que vous faites sur Internet.**4. Évitez les tentatives de phishing**Si vous recevez des e-mails ou des messages prétendant provenir d'une personne proche de vous, de votre banque ou de la police vous demandant de télécharger des pièces jointes douteuses, d'accéder à des liens raccourcis ou de partager des informations sensibles, ignorez-les. Contactez plutôt l'expéditeur présumé pour découvrir la vérité. Essayez de googler des parties du message que vous avez reçu entre guillemets. S'il s'agit d'une escroquerie par hameçonnage, vous êtes susceptible d'obtenir des résultats lorsque d'autres personnes disent avoir reçu le même message.**5. Ne gardez pas le Bluetooth activé**Bien que Bluetooth ait ses utilisations, le garder allumé à tout moment est tout un pari. En 2017, une nouvelle méthode de piratage Bluetooth a été découverte qui affectait des millions d'appareils en permettant aux pirates d'utiliser la menace MITM Man in the Middle pour obtenir les informations de votre appareil. Dans l'ensemble, il vaut mieux être prudent et désactiver Bluetooth lorsque vous ne l'utilisez pas pour garder votre sécurité en ligne intacte.**6. Désactivez les services de localisation sur vos appareils mobiles**Les services de localisation peuvent être vraiment utiles, mais ils peuvent aussi être très risqués, il y a le fait que certaines applications pourraient divulguer votre position. Si cela se produit, cela ne signifie pas que vous serez en danger immédiat. Pourtant, votre sécurité en ligne sera menacée.**7. Utilisez des bloqueurs de scripts dans vos navigateurs**Les bloqueurs de scripts sont des extensions de navigateur que vous pouvez utiliser pour vous assurer que les sites Web auxquels vous accédez n'exécutent pas de scripts et de plug-ins non autorisés en arrière-plan susceptibles de compromettre votre sécurité sur Internet. N'oubliez pas - certains scripts peuvent être si dangereux qu'ils peuvent prendre le contrôle de votre navigateur, tandis que d'autres peuvent exécuter des redirections ou des publicités de phishing, ou même extraire des crypto-monnaies en utilisant votre CPU.**8. Gardez votre système d'exploitation à jour**Ne pas installer les mises à jour les plus récentes sur votre système d'exploitation peut gravement nuire à votre sécurité en ligne. Parce que les acteurs malveillants peuvent utiliser les vulnérabilités potentielles à leur avantage - des vulnérabilités qui auraient pu être corrigées avec la dernière mise à jour.**9. Envisagez d'utiliser des applications de messagerie et des e-mails cryptés**Si vous voulez vraiment vous assurer que vos communications en ligne sont sécurisées, vous pouvez essayer d'utiliser une des différentes applications pour la messagerie. En ce qui concerne les e-mails, c'est la même chose, recherchez en ligne différentes applications et quel type de sécurité elles offrent.**10. Utilisez des mots de passe forts**Avoir des mots de passe puissants pour vos comptes est extrêmement important, mais en trouver un vraiment bon est plus facile à dire qu'à faire.Si vous avez besoin d'aide, mais voici les idées principales :1.Utilisez des espaces si c'est autorisé. 2. N'utilisez que des mots de passe longs. Idéalement, ne vous en tenez pas à un seul mot. 3. N'utilisez pas de mots du dictionnaire comme mot de passe. 4.Utilisez des lettres majuscules et minuscules et mélangez-les au hasard. 5.Utilisez des symboles (comme $, % ou \*) dans votre mot de passe. 6.Incluez des chiffres dans votre mot de passe. 7. Essayez de faire de votre mot de passe une phrase entière. 8.Inversez certains mots que vous utilisez dans le mot de passe (au lieu de "chaise", utilisez "esiahc"). 9. Essayez également de ne pas utiliser le même mot de passe pour tous vos comptes. Il est préférable d'utiliser des mots de passe différents, ou à tout le moins des variantes de votre mot de passe principal. **4.2 Conseils pour la sécurité en ligne dans un contexte culturel**Grâce à Internet, il existe plusieurs façons pour les consommateurs d'obtenir des billets pour un événement à venir. L'inconvénient est qu'il existe également de nombreux pièges que les consommateurs doivent éviter. Cliquer sur le mauvais lien ou faire confiance au mauvais site Web peut entraîner un faux billet et une perte de fonds.Voici quelques conseils pour être en sécurité en ligne, avec un exemple précis d'achat de billets en ligne pour un événement culturel :• Achetez directement sur le site dans la mesure du possible. De nombreux agents de vente de billets officiels proposent désormais également des options de vente secondaires. Ne cliquez pas à partir d'e-mails ou de publicités en ligne ; une astuce courante consiste à créer une adresse Web similaire à celle d'une entreprise bien connue.**• Tenez compte de votre source**. Connaissez la différence entre un courtier de billets professionnel (un revendeur légitime et accrédité), un revendeur de billets (un vendeur de billets non réglementé et sans licence) et un escroc vendant des billets frauduleux.• Connaître la politique de remboursement. Vous devez acheter des billets uniquement auprès d'un revendeur de billets qui fournit des détails clairs sur les conditions de la transaction. Les vendeurs doivent divulguer à l'acheteur, avant l'achat, l'emplacement des sièges représentés par les billets, soit oralement, soit par référence à un plan de salle ; et, si les billets ne sont pas disponibles pour un accès immédiat à l'acheteur, divulguer quand les billets seront expédiés ou seront disponibles pour le ramassage.• Utilisez des modes de paiement assortis d'une protection. Utilisez toujours une carte de crédit, vous avez donc un recours si les billets ne sont pas comme promis. Les cartes de débit, les virements bancaires ou les transactions en espèces sont risqués ; si les billets sont frauduleux, vous ne pourrez probablement pas récupérer votre argent.• Méfiez-vous des publicités. Lorsque vous recherchez des billets en ligne sur le Web, des publicités pour des billets bon marché apparaissent souvent. Faites preuve de bon sens; certaines de ces publicités seront des escroqueries aux billets, surtout si les prix sont bas.• Si vous n'êtes pas sûr, vérifiez vos billets. Visitez l'aréna où se déroule l'événement. Présentez votre ticket au service client et ils pourront vérifier si votre ticket est légitime et vous montrer comment savoir si un ticket est faux.1. **CONCLUSION**

La sécurité en ligne dans un contexte culturel plus large est un sujet très intéressant, le contenu culturel étant largement disponible, il fait également l'objet de menaces en ligne.Les technologies numériques ont révolutionné tous les aspects de nos vies. Ils ont eu un impact sur les chaînes de valeur de toutes les industries culturelles et créatives non seulement en ce qui concerne le processus créatif et son exécution, mais aussi en ce qui concerne la fabrication d'une œuvre ou d'un produit d'art et sa promotion, sa distribution, sa commercialisation et sa vente. Alors que le virage numérique se poursuit, de plus en plus d'artistes, de cinéastes, de producteurs, de musiciens, etc. distribuent leurs produits par voie numérique.À la fin de ce module, vous acquerrez des connaissances sur la reconnaissance des fausses informations nouvelles et manquantes ainsi que sur la sécurité en ligne dans le contexte culturel. En utilisant les conseils et les exemples fournis comme lignes directrices lorsque vous êtes en ligne, vous pouvez renforcer votre sécurité en ligne. Avec les menaces de sécurité telles que les logiciels malveillants, les escroqueries, le phishing, le piratage et la diffusion de fausses informations et de fausses informations de désinformation devenant de plus en plus courantes de nos jours, la sécurité en ligne est devenue plus importante que jamais.Sécurité en ligne ? L'essentiel / Points clésLa sécurité en ligne représente les règles que vous suivez, les actions que vous entreprenez et les processus qui garantissent votre sécurité sur Internet. Avec les menaces de sécurité (malwares, escroqueries, hameçonnage, piratage, etc.) de plus en plus courantes de nos jours, la sécurité en ligne est devenue plus importante que jamais.Habituellement, la meilleure façon de vous assurer que vous êtes en sécurité en ligne est d'utiliser un programme antivirus puissant, un VPN fiable, des mots de passe puissants et des bloqueurs de scripts (entre autres).Les fausses nouvelles font référence à des contrevérités délibérées ou à des histoires qui contiennent une part de vérité mais qui ne sont pas tout à fait exactes, par accident ou à dessein.Certaines personnes prétendent également que les histoires véridiques sont de "fausses nouvelles", simplement parce qu'elles ne sont pas d'accord avec elles. Cela peut conduire à ignorer dangereusement des conseils vitaux.Les fausses nouvelles peuvent avoir un impact négatif sur les aspects sociaux et culturels de la société, il est donc crucial de savoir comment séparer les vraies des fausses nouvelles ainsi que de reconnaître quand il y a des informations manquantes, de la désinformation ou de la désinformation. Vous pouvez le faire en suivant ces six étapes :1. Développer un esprit critique. 2.Vérifiez la source. 3. Voyez qui d'autre rapporte l'histoire. 4.Examinez les preuves. 5.Ne prenez pas les images à leur valeur nominale. 6.Vérifiez qu'il "sonne bien".  |
| **Contenu en puces** |
| * Le contenu culturel est largement accessible sur Internet et ouvert aux menaces en ligne, la diffusion d'informations manquantes, la désinformation, la désinformation et les fausses nouvelles pourraient nuire à l'expérience d'une personne tout en appréciant et en informant sur un spectacle ou un événement culturel.
* La sécurité Internet consiste en une gamme de tactiques de sécurité pour protéger les activités et les transactions effectuées en ligne sur Internet.
* Une menace à la sécurité en ligne fait référence à toute attaque malveillante potentielle qui cherche à accéder illégalement à des données, à perturber des opérations numériques ou à endommager des informations.
* La sécurité en ligne est consciente de la nature des menaces possibles que vous pourriez rencontrer lors de vos activités sur Internet, il peut s'agir de menaces à la sécurité, de la protection et de la gestion de vos données personnelles en ligne et de la prévention des contenus préjudiciables ou illégaux.La sécurité en ligne protège les personnes effectuant des actions en ligne par la sensibilisation, l'éducation, l'information et la technologie.
* Il existe des dizaines de menaces de sécurité en ligne sur Internet, ce module se concentre sur les plus dangereuses et les plus courantes, telles que : les logiciels malveillants ; L'homme du milieu MITM ; Hameçonnage; Attaques de mot de passe, etc.
* Les internautes doivent savoir reconnaître les fake news, la désinformation, la désinformation et se protéger en conséquence.Les fausses nouvelles peuvent avoir un impact négatif sur les aspects sociaux et culturels de la société, il est donc crucial de savoir comment séparer les vraies des fausses nouvelles ainsi que de reconnaître quand il y a des informations manquantes, de la désinformation ou de la désinformation.
 |
| **5 entrées de glossaire** |
| **1) Sécurité en ligne**La sécurité Internet consiste en une gamme de tactiques de sécurité pour protéger les activités et les transactions effectuées en ligne sur Internet.**2) Sécurité en ligne**La sécurité en ligne est consciente de la nature des menaces possibles que vous pourriez rencontrer lors de vos activités sur Internet, il peut s'agir de menaces à la sécurité, de la protection et de la gestion de vos données personnelles en ligne et de la prévention des contenus préjudiciables ou illégaux.La sécurité en ligne protège les personnes effectuant des actions en ligne par la sensibilisation, l'éducation, l'information et la technologie.**3) Contexte culturel**Le contexte culturel est lié à la société dans laquelle les individus sont élevés et à la façon dont la culture affecte le comportement. Elle intègre des valeurs apprises et des attitudes partagées par des groupes de personnes. Il comprend les croyances, les significations, les coutumes, les idées, le langage, les normes.Désigne la signification symbolique, la dimension artistique et les valeurs culturelles qui émanent ou expriment les identités culturelles.**4) Fausses nouvelles**Les fausses nouvelles, souvent à caractère sensationnel, créées pour être largement partagées ou diffusées dans le but de générer des revenus, ou de promouvoir ou de discréditer une personnalité publique, un mouvement politique, une entreprise, etc.**5) Informations manquantes**est une information incomplète ou inexacte qui vise à détourner l'attention d'informations exactes, à semer la confusion ou à modifier le contexte d'une phrase, d'une action, d'une activité, etc. |
| **Bibliographie et autres références** |
| * <https://www.mindtools.com/pages/article/fake-news.htm>
* [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS\_BRI(2021)690570\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI%282021%29690570_EN.pdf)
* <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media>
* <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf>
* <https://www.nature.com/articles/s41586-021-03344-2>
* <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf>
* <https://academicguides.waldenu.edu/library/fakenews/examples>
* [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS\_BRI(2021)690570\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI%282021%29690570_EN.pdf)
* [https://www.europarl.europa.eu/thinktank/en/document/EPRS\_BRI(2021)690570](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282021%29690570)
* <https://en.wikipedia.org/wiki/Fake_news>
* [https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact- de fausses nouvelles](https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news)
* [https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and- pouvons-nous-aider-les-utilisateurs](https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users)
* <https://researchguides.austincc.edu/c.php?g=612891&p=4258046>
 |
| **Cinq questions d'auto-évaluation à choix multiples** | 1) Un e-mail dans votre boîte de réception vous demande de vous connecter avec un mot de passe pour des raisons de sécurité. Qu'est-ce que tu ferais ?1. Rien, je vais ignorer le message
2. Je ferai comme demandé, c'est une raison de sécurité
3. Je vais contacter un expert en informatique pour avoir plus d'informations

**Bonne réponse : A**2) Vous êtes sur un site qui vend des billets gratuits pour un événement culturel près de chez vous. Ils sont gratuits et ne demandent que certaines de vos informations personnelles. Qu'est-ce que tu ferais ?1. Je vais acheter les billets et entrer mes informations personnelles
2. Je vais vérifier le site Web pour voir si c'est réel et si ce n'est pas le cas, puis signaler le site
3. Je partagerai le site pour que d'autres puissent également obtenir les billets

**Bonne réponse : B**3) Vous avez visité une visite virtuelle d'un lieu culturel bien connu. Vous avez remarqué des informations manquantes sur l'un des sites. Qu'est-ce que tu ferais?1. Je remplirai le terrain vide moi-même
2. J'informerai le guide de la visite virtuelle de cette éventuelle erreur
3. je ne ferai rien

**Bonne réponse : B**4) Vous créez un compte sur un site Web et vous devez créer un mot de passe. Quel mot de passe est le plus sécurisé ?1. Votre propre nom
2. Une ligne aléatoire de chiffres et de lettres que vous pourriez écrire sur une feuille de papier pour vous en souvenir
3. Votre numéro de sécurité sociale

**Bonne réponse : B**5) Protégez-vous vos informations personnelles lorsque vous utilisez les réseaux sociaux1. Oui
2. Non
3. Pas certain

**Bonne réponse : Facultatif, toutes les réponses sont correctes** |
| **Matériel connexe** | Comment identifier les informations manquantes et les fausses nouvelles en ligne dans un contexte culturel pertinent\_PPT\_CDI |
| **PPT associés** |  |
| **Lien de référence** |  |
| **Vidéo au format YouTube (le cas échéant)** | <https://youtu.be/vPAW5j_L4-c><https://www.youtube.com/watch?v=0yL-k5nB65o> |