Fiche de formation IWS

|  |  |
| --- | --- |
| **Titre** | **Identité numérique et réputation en ligne** |
| **Zone d'entraînement** | *Veuillez sélectionner une ou plusieurs des options suivantes :*   |  |  | | --- | --- | | Sécurité en ligne |  | | Littérature culturelle et médiatique |  | | Transactions économiques |  | | Protection des données personnelles |  | | Identité numérique et e-réputation | *X* | |
| **Mots clés (balise meta)** | **Identité numérique, réputation en ligne, Internet, fraudes, en ligne, escroquerie, réseaux sociaux** |
| **Fourni par** | **Internet Web Solutions** |
| **Langue** | **Français** |
| **Objectifs / buts / résultats d'apprentissage** | |
| **A la fin de ce module,vous serez en mesure de:**  **Savoir ce que vous devez connaître sur votre identité numérique et votre réputation en ligne.**  **L'unité se concentre sur :**  **Unité 3.1. Docteur Jack et Monsieur Anonyme (Qui êtes-vous et les autres sur Internet et comment le protéger)**  **Section 3.1.1 Introduction**  **Article 3.1.2. Usurpation d'identité : que se passe-t-il s'ils volent votre identité ?**  **Article 3.2.3. Vol de compte : que se passe-t-il s'ils utilisent vos comptes ? Quelques conseils pour l'éviter.**  **Article 3.2.4. Autres conseils** | |
| **La description** | |
| **Cette unité apportera des "faire et ne pas faire” comme"N'utilisez pas d'ordinateurs publics”,"Définissez un mot de passe fort et complexe”,"Assurez-vous que vous utilisez une connexion sécurisée”, authentification à double facteur, etc. pour protéger votre identité numérique. Cette unité parlera également des moyens sûrs d'utiliser les réseaux sociaux et de ce qu’il faut faire pour ne pas vous révéler en ligne.** | |
| **Contenu organisé en 3 niveaux** | |
| **Unité 3.1 Doctor Jack et Mister Hyde (Qui êtes-vous et les autres sur Internet et comment le protéger)**  **Section 3.1.1 Introduction**  Sur Internet, vous êtes tout ce que vous publiez et tout ce que vous commentez aux autres utilisateurs.  Tout ce que vous publiez en ligne peut être vu par les autres utilisateurs.  Même si vous pouvez définir les paramètres de confidentialité lorsque vous publiez sur "amis uniquement" ou similaire, une personne qui souhaite voir votre message a des moyens de l'obtenir.  Non parce que les gens ne peuvent pas vous voir, vous pourriez agir différemment parce que vous êtes derrière un écran.  Contrairement à la vraie vie, tout ce que vous publiez sur Internet a une visibilité mondiale.  Cela signifie que des personnes du monde entier peuvent en savoir plus sur vous, et de même, vous pouvez en savoir plus sur des personnes du monde entier.  Un escroc peut rechercher beaucoup plus de personnes et choisir sa victime avec plus de soin. Ceci et d'autres facteurs rendent les escroqueries en ligne de plus en plus courantes.  **Article 3.1.2. Usurpation d'identité : que se passe-t-il s'ils volent votre identité ?**  Une personne qui accède illégalement à votre compte peut effectuer de nombreuses actions malveillantes.  Au mieux, ils peuvent se faire passer pour vous pour publier des messages compromettants ou illégaux.  Au pire, ils peuvent se faire passer pour vous et parler à vos connaissances ou à votre famille, en leur disant que vous avez un problème et que vous avez besoin d'argent, les arnaquant ainsi. L'usurpation d'identité ne concerne pas que vous.  Un autre mauvais cas est que si quelqu'un a accès à vos coordonnées bancaires, il pourrait commencer des achats ou des transactions en ligne et voler de l'argent.  Si jamais cela se produit, essayez de parler au support de la plateforme où votre compte a été volé, changez les mots de passe, informez les personnes concernées, et si le voleur a pu effectuer un achat, informez également votre banque.  L'usurpation d'identité ne concerne pas que vous !  **Section 3.2.3 Vol de compte : que se passe-t-il s'ils utilisent vos comptes ?**  Un autre mauvais cas est que si quelqu'un a accès à vos coordonnées bancaires, il pourrait commencer des achats ou des transactions en ligne et voler de l'argent.  Si jamais cela se produit, essayez de parler au support de la plateforme où votre compte a été volé, changez les mots de passe, informez les personnes concernées, et si le voleur a pu effectuer un achat, informez également votre banque.  Il y a plusieurs choses que vous pouvez faire pour éviter le vol de compte :  -Ne pas enregistrer les mots de passe sur n'importe quel appareil, essayez de vous en souvenir.  -Essayez d'utiliser différents mots de passe pour différents sites. Si quelqu'un découvre votre mot de passe pour une plate-forme, il ne pourra pas accéder aux autres sites.  -N'utilisez pas votre nom, votre nom d'utilisateur ou d'autres informations personnelles sur la plate-forme qui facilitent la recherche.  -Utilisez des mots de passe de plus de 8 caractères et utilisez un chiffre ou un caractère spécial pour éviter les attaques par force brute pour découvrir votre mot de passe.  Ne partagez jamais votre mot de passe en ligne, même si une personne vous dit qu'elle est modérateur, administrateur ou personnel d'assistance d'un site.  **Article 3.2.4. Autres conseils**  En effet, vous devez également faire plus attention à ce que vous publiez sur les réseaux sociaux.  Essayez de publier le moins d'informations possible sur vous-même, en particulier des informations sensibles, des détails d'identification,ou coordonnées bancaires.  Les informations importantes que vous ne devez PAS partager publiquement peuvent être :  -Le lieu où vous habitez  -Adresse e-mail  -Numéro de téléphone  - contenu multimédia compromettant  -Documents personnels  -Informations sur vos opérations bancaires  -Informations salariales  -Mots de passe de toute nature  Usurpation de compte et d'identité  Évitez de vous connecter à des comptes sur les ordinateurs d'autres personnes, en particulier les ordinateurs publics.  De nombreuses plateformes prennent en charge l'authentification en deux étapes, par exemple en utilisant votre numéro de téléphone, utilisez-le lorsque vous en avez l'occasion.  Ce qui est en ligne reste en ligne pour toujours. Ce que vous publiez, ce que vous dites, comment vous vous comportez, sera accessible à tous, y compris : les futurs employeurs potentiels, votre famille, vos enfants et vos amis. Et pas seulement maintenant, aussi dans le futur | |
| **Contenu en puces** | |
| * **Essayez de publier le moins d'informations possible sur vous-même, en particulier des informations sensibles, des détails d'identification,ou coordonnées bancaires.** * **Ce qui est en ligne reste en ligne pour toujours. Ce que vous publiez, ce que vous dites, comment vous vous comportez, sera accessible à tous, y compris : les futurs employeurs éventuels, votre famille et vos enfants,et vos amis. Et pas seulement maintenant, aussi à l'avenir.** * **Utilisez des mots de passe de plus de 8 caractères et utilisez un chiffre ou un caractère spécial pour éviter les attaques par force brute pour découvrir votre mot de passe.** | |
| **5 entrées de glossaire** | |
| **Identité numérique :**  *L'identité numérique est souvent utilisée de manière à ce que les données sur les personnes stockées dans des systèmes informatiques soient liées à leur identité civile ou nationale.*  **Réputation en ligne :**  *C'est la réputation d'une entreprise, d'une personne, d'un produit, d'un service,ou tout autre élément sur Internet et les plateformes numériques.*  **Authentification en deux étapes :**  *Il s'agit d'une méthode d'authentification électronique dans laquelle un utilisateur n'a accès à un site Web ou à une application qu'après avoir présenté avec succès deux ou plusieurs éléments de preuve (ou facteurs) à un mécanisme d'authentification.*  **Vol d'identité:**  *La pratique frauduleuse consistant à utiliser le nom et les informations personnelles d'une autre personne afin d'obtenir du crédit, des prêts, etc.*  **Arnaque :**  *Un escroc peut rechercher beaucoup plus de personnes et choisir sa victime avec plus de soin. Ceci et d'autres facteurs rendent les escroqueries en ligne de plus en plus courantes.* | |
| **Bibliographie et autres références** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)  [**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)  [**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **Cinq questions d'auto-évaluation à choix multiples** | 1. Sur Internet:   A. Seules les personnes que vous connaissez peuvent vous trouver  B. Seuls les escrocs peuvent vous trouver  C. Les gens du monde entier peuvent vous trouver  **Correct: C**  2) A quoi sert une usurpation d'identité ?  A. Une usurpation d'identité n'accède qu'à vos coordonnées bancaires  B. Un usurpateur d'identité vient chez vous et vole votre ordinateur portable  C. Un vol d'identité accède à votre compte et effectue des actions malveillantes  **Correct: C**  3) Quelles sont les informations personnelles qu'il est déconseillé de publier sur Internet ?  A. Votre pointure  B. Votre numéro de téléphone  C. Votre profil Facebook  **Correct: B**  **4**) Mot de passe et sécurité. Laquelle des affirmations suivantes est vraie ?  A. Il est préférable de ne pas enregistrer le mot de passe sur n'importe quel appareil  B. Utilisez un mot de passe de moins de 8 caractères  C. Utilisez votre numéro de téléphone comme mot de passe  **Correct: UNE**  5) Pourquoi est-il si important d'éviter de se connecter sur les ordinateurs d'autres personnes ?  R. Parce que c'est impoli  B. Pour protéger votre mot de passe  C. Pour protéger votre identité numérique  **Correct : A** |
|  |  |
| **PPT associés** | [**SOS créativité Module 3 Identité numérique et e-réputation**](http://ppts/SOS%20creativity%20Module%203%20Digital%20Identity%20and%20Online%20Reputation.pptx) |
| **Lien de référence** |  |
| **Vidéo au format YouTube (le cas échéant)** |  |