Fiche de formation IWS

|  |  |
| --- | --- |
| **Titre** | **Sécurité en ligne et créativité : quoi de neuf ?** |
| **Zone d'entraînement** | *Veuillez sélectionner une ou plusieurs des options suivantes :*

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

 |
| **Mots clés (balise meta)** | **Escroqueries, fraudes, conseils de sécurité en ligne, Internet** |
| **Fourni par** | **Internet Web Solutions**  |
| **Langue** | **Français** |
| **Objectifs / buts / résultats d'apprentissage** |
| **À la fin de ce module, vous serez en mesure de prendre conscience de la sécurité en ligne dans le monde culturel numérique. Cette unité portera sur :****Unité 2.1 Escroqueries en ligne les plus courantes : exemples des escroqueries en ligne les plus courantes, protégeant vos informations en ligne.*** **Article 2.1.1. introduction**
* **Article 2.1.2. Offre d'emploi**
* **Article 2.1.3. Arnaque bancaire**
* **Article 2.1.4. Shopping en ligne**
* **Article 2.1.5. Produits tiers**
* **Article 2.1.6. Héritage via WhatsApp**
* **Article 2.1.7. SMS frauduleux de votre banque**
* **Article 2.1.8. Escroquerie à la loterie**
* **Article 2.1.9. Faux organismes de bienfaisance**

**Unité 2.2. Sécurité en ligne dans le monde culturel, comment éviter les arnaques propres au monde culturel (faux billets, piratage ou hameçonnage)*** **Section 2.2.1 Comment fonctionnent les escrocs**
* **Article 2.2.2. Mesures pour vous protéger**
* **Unité 2.3. Conseils de sécurité en ligne**
* **Article 2.3.1. Comment configurer un mot de passe sécurisé**
 |
| **La description** |
| **Ce cours s'adresse aux adultes,** qui apprennent les bases d'Internet. Le module développera les concepts de base nécessaires pour évaluer et protéger les systèmes de sécurité de l'information afin de sensibiliser les utilisateurs numériques tardifs aux escroqueries ou fraudes potentielles qu'ils pourraient rencontrer sur le Web lors de l'utilisation ou de la recherche de ressources culturelles. Cette unité d'apprentissage enseignera aux personnes âgées comment détecter les escroqueries financières les plus courantes en ligne et comment protéger leurs informations financières et leurs comptes. |
| **Contenu organisé en 3 niveaux** |
| Module 2 : Sécurité en ligne et créativité : quoi de neuf ?**Unité 2.1 Escroqueries en ligne les plus courantes : exemples des escroqueries en ligne les plus courantes, protégeant vos informations en ligne.****Article 2.1.1. introduction**Escroqueries en ligne les plus courantes : exemples des escroqueries en ligne les plus courantes, protégeant vos informations en ligne.La fraude sur Internet devient de plus en plus courante en raison du nombre croissant de personnes qui utilisent Internet quotidiennement.Ces escroqueries veulent non seulement votre argent, mais elles veulent aussi vos informations, et ces dernières sont plus difficiles à détecter.Le fonctionnement de base des escrocs n'a pas changé, ils proposent des produits ou des services en échange d'une somme d'argent "trop ​​belle pour être vraie" ou en échange de quelques questions pour obtenir des informations.Ils peuvent également proposer des prêts ou des offres d'emploi pour vous inciter à mordre à l'hameçon.**Article 2.1.2. Offre d'emploi**Par exemple, une offre d'emploi propose un salaire à temps plein uniquement avec des horaires journaliers à temps partiel et ne nécessite aucune expérience préalable. Le salaire est trop élevé, et cela pourrait être considéré comme une première indication que l'annonce pourrait être une arnaque.Avant de remplir le formulaire ou de fournir des informations, il est toujours bon :- de vérifier l'authenticité du site internet sur lequel l'annonce est publiée* la qualité des images ou des commentaires en cas de vente de produits
* la société qui publie l'annonce
* les allocations de travail offertes

**Article 2.1.3. Arnaque bancaire**D'autres tentatives de fraude peuvent usurper l'identité d'une entité telle que votre banque ou un site que vous fréquentez sous prétexte qu'il existe une offre intéressante ou qu'il y a un problème avec un lien suspect.Si vous pensez que cela pourrait être important, comme dans le cas de votre banque, appelez-les au lieu de cliquer sur le lien.**Article 2.1.4. Shopping en ligne**Les achats en ligne sont de plus en plus courants, alors voici quelques conseils pour acheter en ligne en toute sécurité.- Le site Web doit avoir une connexion cryptée sécurisée, le protocole Web doit être https. Le cryptage permet de masquer des informations afin qu'elles ne puissent pas être lues sans connaissances particulières (comme un mot de passe). Cela se fait avec un code secret ou un chiffrement. Les informations cachées sont dites cryptées.- Assurez-vous que vous êtes sur un site Web de confiance. Un site Web qui propose des prix anormalement bas, tous les prix sont identiques, aucune critique ou des images de produits suspects indiquent que le site Web est une arnaque.**Article 2.1.5. Produits tiers**Certains sites Web vendent des produits tiers. Dans ces cas, vous devez également enquêter sur la société d'où provient le produit.* C'est un bon signe si le site affiche clairement les informations de coût et d'expédition, accepte plusieurs modes de paiement et envoie une facture d'achat.

- Si vous pensez que le site est authentique et que vous effectuez un achat, n'enregistrez jamais les informations de votre carte de crédit. Cela empêchera quelqu'un d'accéder à votre appareil et de faire des achats non désirés.* Vérifiez périodiquement votre solde et si vous constatez des mouvements suspects, signalez-les rapidement à votre banque.

- Si le produit n'arrive pas, essayez de contacter le vendeur ou la plateforme où il est vendu.**Article 2.1.6. Héritage via WhatsApp**Sur WhatsApp une personne vous parle en vous disant qu'elle est très âgée et qu'elle a un héritage sans héritiers, et vous propose d'en hériter vous-même.Une autre personne vous parle directement d'une astuce pour investir sans risque en vous promettant de gagner 100 000 € en un mois seulement.Homme/femme séduisant(e) amoureux(se) de vousUne personne avec une photo attrayante que vous ne connaissez pas du tout essaie de vous parler et vous parle de sujets suggestifs.Méfiez-vous des personnes que vous rencontrez en ligne depuis l'étranger.Apprenez les signes d'une arnaque relationnelle. Sachez quoi surveiller.N'envoyez jamais d'argent.Si vous leur avez déjà donné de l'argent, n'allez pas à l'étranger pour essayer de le récupérerConfirmez toujours leur identité et leur légitimité avant de vous rendre à l'étranger pour les rencontrer.**Article 2.1.7. SMS frauduleux de votre banque**Un SMS arrive sur votre téléphone portable de votre supposée banque disant qu'il y a une erreur avec votre compte bancaire, et vous devez remplir un formulaire.Une personne se fait passer pour un modérateur d'un réseau social et vous demande de lui donner votre mot de passe pour régler un problème.Sur un site Web d'offres d'emploi tiers, ils offrent le double du montant d'un salaire normal.Lorsque vous essayez d'effectuer un achat auprès d'un particulier, il vous demande de lui verser l'argent avant de pouvoir expédier le produit, ou il ne peut vous donner aucune information sur l'expédition.**Article 2.1.8. Escroquerie à la loterie**Une escroquerie à la loterie est un type de fraude à l'avance qui commence par une notification inattendue par e-mail, un appel téléphonique ou un envoi postal (incluant parfois un gros chèque) expliquant que "Vous avez gagné!" une grosse somme d'argent dans une loterie. Le destinataire du message - la cible de l'escroquerie - est généralement invité à garder l'avis secret, "en raison d'une confusion dans certains noms et numéros", et à contacter un "agent de réclamation". Après avoir contacté l'agent, la cible de l'escroquerie se verra demander de payer des "frais de traitement" ou des "frais de transfert" afin que les gains puissent être distribués, mais ne recevra jamais de paiement de loterie.**Article 2.1.9. Faux organismes de bienfaisance**Les escrocs se font passer pour de véritables organismes de bienfaisance et demandent des dons ou vous contactent en prétendant collecter de l'argent après des catastrophes naturelles ou des événements majeurs.Les faux organismes de bienfaisance essaient de profiter de votre générosité et de votre compassion pour les personnes dans le besoin. Les escrocs voleront votre argent en se faisant passer pour un véritable organisme de bienfaisance.Non seulement subir ces escroqueries vous coûte de l'argent, mais elles détournent également des dons indispensables d'organismes de bienfaisance et de causes légitimes.Les fausses approches caritatives se produisent toute l'année et prennent souvent la forme d'une réponse à de véritables catastrophes ou urgences, telles que des inondations, des cyclones, des tremblements de terre et des feux de brousse.**Unité 2.2. Sécurité en ligne dans le monde culturel, comment éviter les arnaques propres au monde culturel (faux billets, piratage ou hameçonnage)****Section 2.2.1 Comment fonctionnent les escrocs**Les escrocs peuvent :* créer de faux sites Web
* utiliser des sites Web authentiques pour publier de fausses annonces pour un billet de concert et un laissez-passer pour le musée
* proposer de faux forfaits d'entrée et de billets VIP

Pour éviter une arnaque au ticket :* faites un choix réfléchi lorsque vous consultez le site Web du revendeur de billets
* utiliser un site Web réputé

Il existe des revendeurs de billets légaux, mais si une offre semble trop belle pour être vraie, c'est probablement le cas.**Article 2.2.2. Mesures pour vous protéger*** Faites preuve de bon sens avant de transmettre des informations sensibles.
* Ne faites jamais confiance aux messages alarmants.
* N'ouvrez pas les pièces jointes de ces e-mails suspects ou étranges, en particulier les pièces jointes Word, Excel, PowerPoint ou PDF.
* Utilisez un site Web réputé

**Unité 2.3. Conseils de sécurité en ligne*** Une fois que vous avez un compte de réseau social, vous pouvez l'utiliser uniquement pour parler à des personnes que vous connaissez dans la vraie vie et publier des opinions ou des photos (mieux sans données sensibles).

**Article 2.3.1. Comment configurer un mot de passe sécurisé**Veillez toujours à respecter les conditions d'utilisation du site et à ne pas commettre d'actes répréhensibles.1. Arrêtez de croire à des images inconnues. Vous devriez arrêter de croire les images comme les chats et les captures d'écran.
2. Ne cliquez pas sur des pièces jointes inconnues.
3. Vérifiez la source de vos messages.
4. Ne partagez jamais de données personnelles.
5. Méfiez-vous des arnaques possibles.
6. Protégez vos données financières.
7. Évitez de partager des détails de base.
8. Utilisez des mots de passe ou des codes PIN avec des caractères tels que &, \*. \_\_, minuscule et MAJUSCULE.
 |
| **Contenu en puces** |
| * **Utilisez des mots de passe ou des codes PIN avec des caractères tels que &, \*. \_\_, minuscule et MAJUSCULE**.
* **Une fois que vous avez un compte de réseau social, vous pouvez l'utiliser uniquement pour parler à des personnes que vous connaissez dans la vraie vie et publier des opinions ou des photos (mieux sans données sensibles).**
* **Les fausses approches caritatives se produisent toute l'année et prennent souvent la forme d'une réponse à de véritables catastrophes ou urgences, telles que des inondations, des cyclones, des tremblements de terre et des feux de brousse.**
* **Une escroquerie à la loterie est un type de fraude à l'avance qui commence par une notification inattendue par e-mail, un appel téléphonique ou un envoi postal (incluant parfois un gros chèque) expliquant que "Vous avez gagné!" une grosse somme d'argent dans une loterie.**
 |
| **5 entrées de glossaire** |
| **Arnaque à la loterie :** *Une escroquerie à la loterie est un type de fraude à l'avance qui commence par une notification inattendue par e-mail, un appel téléphonique ou un envoi postal (incluant parfois un gros chèque) expliquant que "Vous avez gagné!" une grosse somme d'argent dans une loterie.***Fausse charité :** *type de fraude qui se produit lorsque des organisations caritatives sollicitent des fonds auprès du public à des fins philanthropiques, telles que la recherche de remèdes contre des maladies ou l'aide aux familles de policiers tués.***Produits tiers :** *désigne tout produit et/ou service d'un tiers qui est proposé par ou par l'intermédiaire de la Banque.***Escroquer:***Une escroquerie ou un tour de confiance est une tentative d'escroquerie d'une personne ou d’un groupe en gagnant sa confiance.***Hameçonnage:***L'hameçonnage est un type d'ingénierie sociale dans lequel un attaquant envoie un message frauduleux (par exemple, usurpé, faux ou autrement trompeur) conçu pour tromper une victime humaine afin qu'elle révèle des informations sensibles à l'attaquant ou pour déployer un logiciel malveillant sur l'infrastructure de la victime comme un rançongiciel.* |
| **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) Quels sont les signaux d'alerte pour repérer une arnaque bancaire ?A. Un lien suspect reçu par emailB. Un e-mail officiel de votre banqueC. Un e-mail d'une association caritative**Correct : A** 2) Que faire si vous êtes victime d'une arnaque bancaire ?A) Fournissez vos informations personnellesB) Cliquez sur les pièces jointes inconnuesC) Appelez la banque pour vérifier le problème**Correct : C**3) Comment éviter une arnaque au ticket ?A) Évitez d'acheter des billets en ligneB) Achetez uniquement sur un revendeur officiel en ligneC) Utiliser un site Web de revendeur de billets suspect**Correct : B**4) À quoi ressemblent les fausses approches caritatives ?A) Ils prennent souvent la forme d'une réponse à une véritable demande d'aide d'un proche vérifié.B) Ils prennent souvent la forme d'une réponse à une véritable demande d'aide d'un ami de la famille vérifiéC) Ils prennent souvent la forme d'une réponse aux catastrophes ou aux urgences, telles que les inondations, les cyclones, les tremblements de terre et les feux de brousse.**Bonne réponse : C**5) Comment configurer un mot de passe sécurisé ?A) Utiliser votre adresseB) Utiliser votre nom completC) En utilisant des caractères tels que &, \*. \_\_, minuscule et MAJUSCULE.**Bonne réponse : C** |
| **Matériel connexe** |  |
| **PPT associés** | [**SOS créativité Module 2 Sécurité en ligne et créativité quoi de neuf**](http://ppts/SOS%20creativity%20Module%202%20Online%20security%20and%20creativity%20what%E2%80%99s%20up.pptx) |
| **Lien de référence** |  |
| Vidéo au format YouTube (le cas échéant) | Sécurité en ligne pour les adultes, Bristol City Council Skills & Learning - Adult & Community Learning Service[**https://www.youtube.com/watch?v=iCs3aJYXLwo**](https://www.youtube.com/watch?v=iCs3aJYXLwo) |