Gros plan d’un logo

Description générée automatiquement

Plan de leçon

Module 6

# Plan de leçon – Module 6

## Résultats d’apprentissage

|  |  |  |  |
| --- | --- | --- | --- |
|  | **CONNAISSANCE** | **COMPÉTENCES** | **ATTITUDES** |
| **Module 6: MENACES EXTERNES ET PARAMÈTRES DE CONFIDENTIALITÉ ET CONTRÔLE PARENTAL SUR LES MÉDIAS SOCIAUX** | Définir le concept de trouble de l’information (voir module 3, atelier 1). | Capacité d’identifier les différents types d’informations et les formes qu’elles peuvent prendre (voir Module 3, Atelier 1). | Sensibilisation à l’importance de l’éducation aux médias afin d’adopter une position active à l’égard de la consommation et de la création de médias. |
| Comprendre ce qu’est un faux compte.  Comprendre la différence entre les faux comptes créés par des humains et leurs objectifs et les faux comptes créés par des logiciels et leurs objectifs.  Définir le concept d’escroquerie et ses objectifs.  Définir les principales caractéristiques d’une arnaque. | Capacité à expliquer ce qu’est un faux compte et ce qu’il vise à réaliser (trolling, satire, arnaque, diffusion de désinformation; certains faux comptes sont gérés par des robots et fonctionnent 24h/24 et 7j/7).  Capacité d’identifier entre un faux compte géré par un bot (et ses objectifs), un faux compte géré par un humain (et ses objectifs) et un bot qui ne vise pas à être confondu avec un faux compte.  Capacité d’expliquer ce qu’est une arnaque et d’identifier une tentative d’escroquerie tout en naviguant dans des environnements numériques.  Capacité d’identifier une arnaque en utilisant plusieurs caractéristiques des escroqueries comme référence (adresse e-mail, contact non sollicité ou inattendu, trop beau pour être vrai, demande de données personnelles, demande de décision rapide, concours aléatoire). | Savoir que les faux comptes peuvent rendre la navigation dans les environnements numériques plus difficile et dangereuse.  Reconnaître que différents types de faux comptes ont des objectifs différents et l’importance de pouvoir les différencier.  Reconnaître que, par définition, les escroqueries sont des tentatives de tromper quelqu’un avec un but ultime (malveillant), comme voler de l’argent.  Déployer la pensée critique et les connaissances acquises pour vous protéger, vous et votre famille, contre les escroqueries. |
| Définir le concept de vol d’identité et énumérer les moyens par lesquels les voleurs d’identité mettent la main sur vos données personnelles.  Connaître les moyens de protéger les données personnelles contre le vol d’identité. | Capacité d’expliquer le terme de vol d’identité, ainsi que de décrire les différentes façons (violations de données, navigation non sécurisée, dark web, etc.)que l’on peut être victime de vol d’identité.  Appliquer différentes façons de protéger les données personnelles en ligne (surveiller les rapports de crédit, les transactions bancaires non autorisées, cesser de recevoir des factures, etc., contacter les autorités, mettre en place une alerte à la fraude). | Reconnaître qu’il est impossible de prouver complètement les données de quelqu’un en ligne, cependant, la connaissance et la surveillance fréquente des comptes peuvent contribuer grandement à la protection des données personnelles dans les environnements numériques.  Reconnaître le risque inhérent de faire des affaires en ligne et d’appliquer des méthodes pour protéger les données personnelles. |
| Définir le concept de matériel pédopornographique (CSAM) (également connu sous le nom de pornographie juvénile, mais évitez d’utiliser ce terme car il est inexact et vise à légitimer l’exploitation des enfants). | Capacité d’expliquer le terme CSAM et les conséquences de l’utilisation de ce matériel en ligne. | Reconnaître que le CSAM est une version moderne de la maltraitance et de l’exploitation des enfants en ligne, qui est également en augmentation. Assumer sa responsabilité personnelle et rapporter le matériel CSAM et être conscient de la façon d’aider un ami qui a des pensées ou un comportement inappropriés. |
| Définir le concept d’abus en ligne.  Définir le concept de cyberintimidation.  Définir le concept d’autres formes d’abus en ligne et les moyens d’y remédier. | Capacité d’expliquer et d’identifier les différents types d’abus en ligne (cyberintimidation, abus émotionnel, toilettage, sexting, abus sexuel et exploitation).  Capacité d’expliquer et d’identifier la cyberintimidation lorsqu’elle se produit dans des environnements en ligne.  Capacité d’identifier plusieurs types d’abus en ligne et d’appliquer des mesures dans le but d’y remédier (par exemple, sur le sexting). | Reconnaître que les abus peuvent également avoir lieu en ligne et ayez confiance en vos capacités à les identifier.  Reconnaître que la cyberintimidation est un terme de harcèlement qui se produit spécifiquement en ligne (également connu sous le nom d’intimidation en ligne ou de harcèlement en ligne).  Sentez-vous confiant d’informer un membre de la famille des formes de violence qu’ils peuvent rencontrer ou dont ils peuvent être témoin en ligne, ainsi que des moyens de les combattre. |
| Définition du concept de paramètres de confidentialité.  Connaître le cadre juridique européen sur la protection des données personnelles des personnes (Règlement général sur la protection des données 2016/679). | Possibilité d’expliquer le terme « paramètres de confidentialité » et les moyens d’ajuster ces paramètres afin de protéger la vie privée en ligne (profil privé, ne pas accepter les demandes de personnes aléatoires, ne pas partager de mot de passe, rendre les messages visibles uniquement par des amis, etc.).  Capacité à décrire les principales responsabilités des plateformes de médias sociaux et des entreprises en ligne conformément au RGPD lors de la collecte, du partage de données personnelles et de la communication globale avec le client. Les déclarations de politique de confidentialité fournissent des informations détaillées sur la gestion des données personnelles. | Reconnaître que la plupart des plateformes de médias sociaux offrent la possibilité de personnaliser son exposition en ligne.  Avoir confiance dans l’application de mesures de sécurité (par exemple, mot de passe d’authentification à deux facteurs) et de confidentialité dans divers environnements numériques. |
| Définir le concept de contrôle parental dans le monde numérique.  Définir les types de contrôle parental que l’on peut appliquer sur les médias sociaux.  Connaître plusieurs façons d’appliquer le contrôle parental sur plusieurs plateformes de médias sociaux. | Capacité d’expliquer et d’appliquer le contrôle parental à plusieurs environnements (par exemple, télévision, ordinateur, jeux vidéo, etc.).  Capacité à expliquer les différents types de contrôle parental (filtres de contenu, contrôles d’utilisation, outils de gestion de l’utilisation de l’ordinateur et surveillance).  Possibilité d’appliquer le contrôle parental sur plusieurs plateformes de médias sociaux et de savoir quelles plateformes offrent des options limitantes sur le contrôle parental. | Reconnaître que le contrôle parental est nécessaire pour assurer une expérience adaptée aux enfants dans le monde en ligne.  Reconnaître la capacité des parents à limiter l’exposition de leurs enfants à des contenus indésirables.  Se sentir confiant de savoir comment appliquer le contrôle parental sur les médias sociaux pour encourager une expérience sûre et adaptée aux enfants dans les médias sociaux. |

**Le module 6 est divisé en deux ateliers de 2 heures chacun. Le processus d’apprentissagedu module 6 compte également sur 4 heures d’apprentissage autodirigé.**

# Plan de leçon

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Contenu- Description | Méthode d’instruction | Durée | Matériel/équipement requis | Conseils / Astuces | Évaluation | Lectures complémentaires/ Lien vers les ressources |
| Introduction | Bienvenue aux participants. Ils devraient tous se connaître en ce moment, mais vous pouvez lancer un tour de présentation, en commençant par vous-même, en annonçant votre prénom et votre profession / toute information pertinente sur vous-même.  Ensuite, présentez le sujet de ce module: la menace externe des médias sociaux.  Vous pouvez demander aux participants ce qu’ils pensent lorsqu’ils parlent de ce sujet, écrire les mots clés sur le Paperboard. | 15mn | Paperboard  Marqueurs | Le moment d’introduction doit être aussi convivial que possible. Tous les participants devraient sentir qu’ils passeront un bon moment alors... souriez beaucoup! | N/A | N/A |
| Module 6 – Atelier 1 : Menaces externes | Ensuite, expliquez aux participants que nous nous concentrerons sur 3 sujets principaux:   * Faux comptes * Vols d’identité * Abus en ligne   Rappelez-leur que le sujet « Désordres de l’information » a été abordé dans les modules précédents mais qu’il constitue également une menace lorsque l’on est en ligne. Il est également abordé dans les ressources d’apprentissage autodirigées   1. **Catfishing (30mn)**   Commencez par demander aux participants s’ils savent ce qu’est le catfishing.  Montrez ensuite cette courte vidéo pour présenter le concept:  <https://www.youtube.com/watch?v=JPuaOCiVAh0>  Maintenant que les participants savent ce que c’ est, montrez-leur une autre vidéo fournissant des conseils pour repérer les faux profils en ligne (commencez la vidéo à 3mn59 et arrêtez-la à 6mn32):  <https://www.youtube.com/watch?v=LagwG7bieEA>  Voici la liste des outils à utiliser pour le catfishing :   * Recherche d’images inversée Google * Demandez plus d’informations et un selfie   Ensuite, commencez une discussion avec les participants :   * Quels sont les objectifs des catfish? (vol d’identité, argent, solitude, etc.) * Comment éviter que vos proches ne soient victimes des catfish? * En tant que parent, que pouvez-vous faire pour prévenir ces situations?   Affichez la section du PPT « Éviter catfishing ».   1. **Vol d’identité (30mn)**   Le vol d’identité peut être le but du catfishing. C’est un abus courant sur Internet.  Commencer à montrer aux participants cette courte vidéo:  <https://www.youtube.com/watch?v=xnjFb68r29w&ab_channel=GreatLakes>  Pour éviter le vol d’identité et avoir un comportement en ligne sûr, nous devons respecter des règles simples. Affichez la section « Comportements en ligne sûrs » du PPT.  Ensuite, commencez une discussion avec le groupe sur le vol d’identité. Expliquez au groupe que ces escroqueries ciblent également les utilisateurs plus âgés et que cela concerne tous les membres de la famille.  Demandez au groupe s’il a déjà été approché par des escrocs.  Discutez des techniques utilisées pour voler des données :   * Hameçonnage: pratique frauduleuse d’envoi de courriels prétendant provenir d’entreprises réputées afin d’inciter les individus à révéler des informations personnelles * Pharming: acte criminel de produire un faux site Web et de rediriger ensuite les utilisateurs vers celui-ci * Vishing: passer des appels téléphoniques ou laisser des messages vocaux prétendant être d’entreprises réputées afin d’inciter les individus à révéler des informations personnelles * Smishing: envoi de messages texte prétendant être d’entreprises réputées afin d’inciter les individus à révéler des informations personnelles   Demandez au groupe d’échanger des expériences sur ces pratiques et sur la façon dont ils s’en sont remis.   1. **Abus en ligne (30mn)**   Vous allez maintenant discuter du cauchemar de tous les parents: les abus en ligne.  Commencez par la section PPT « Abus en ligne ».  Grâce à la présentation, les participants avaient compris que l’écoute active est l’une des principales qualités des parents de ne rien manquer et de pouvoir détecter les problèmes.  L’activité suivante durera 10mn et sera un brainstorming sur l’écoute active.  Demandez aux participants quelles sont les compétences d’un auditeur actif, prenez des notes sur le Paperboard; assurez-vous que les termes suivants découlent de la conversation :   * Neutre * Sans jugement * Patient * Communication verbale et non verbale * Poser des questions * Réfléchir à ce qui est dit * Demander des éclaircissements * Résumer   **Conclusion**  Enfin, demandez aux parents ce qu’ils ont appris aujourd’hui et s’ils utiliseront ces connaissances à la maison. | 30mn  15mn | PC/Ordinateur portable  Projecteur  Atelier PPT 1  PC/Ordinateur portable  Projecteur  Papier et stylo pour que les participants prennent des notes  Section PPT « Éviter le catfishing »  PC/Ordinateur portable  Projecteur  Section PPT " Comportements en ligne sûrs »  PC/Projecteur  Ordinateur portable  Section PPT « Abus en ligne »  Paperboard  Marqueurs |  | N/A | N/A |
| Module 6 – Atelier 2 | **Bienvenue**  Accueillez les participants, expliquez les principaux résultats d’apprentissage de l’atelier précédent et faites-leur savoir que cette session se concentrera sur les paramètres de confidentialité et le contrôle parental sur les médias sociaux.  Commencez l’atelier en montrant cette courte vidéo :  <https://www.youtube.com/watch?v=UhhYSrUHnao&ab_channel=TechnologyServicesatIllinois>  Cette vidéo illustre le nombre de données qui peuvent être récupérées à partir de publications simples sur les médias sociaux.  Ensuite, montrez cette vidéo qui présentera le règlement européen sur les données personnelles (RGPD) :  <https://www.youtube.com/watch?v=acijNEErf-c&ab_channel=Channel4News>  Les paramètres de confidentialité sont un moyen de contrôler qui voit les informations vous concernant.  Ensuite, affichez la section PPT « Paramètres de confidentialité »  Assurez-vous que les participants peuvent poser leurs questions.  Afficher la section PPT « Contrôle parental »  Assurez-vous que les participants peuvent poser leurs questions.  Enfin, montrez aux participants la vidéo suivante présentant le logiciel de contrôle parental:  <https://www.youtube.com/watch?v=9DSAi4q6SmQ&ab_channel=10BestOnes>  Demandez aux participants leurs commentaires. Pensent-ils qu’avoir un tel logiciel est une bonne idée? Qu’en est-il de la vie privée de l’enfant? Comment assurer la confiance mutuelle ? | 10mn  5mn  10mn  35mn  30mn  15mn | N/A  PC/Ordinateur portable  Projecteur  PPT Atelier 2  Papier et stylo pour que les participants prennent note  PC/Ordinateur portable  Projecteur  Papier et stylo pour que les participants prennent note  PC/Ordinateur portable  Projecteur  Section PPT « Paramètres de confidentialité »  Papier et stylo pour que les participants prennent note  PC/Ordinateur portable  Projecteur  Section PPT « Contrôle parental »  Papier et stylo pour que les participants prennent note  PC/Ordinateur portable  Projecteur | N/A | N/A | N/A |
| Conclusion | **Conclusion et évaluation du module 6**  Enfin, demandez aux parents ce qu’ils ont appris aujourd’hui et s’ils utiliseront ces connaissances à la maison.  Demandez-leur si le module 6 a répondu à leurs besoins et s’ils ont des questions supplémentaires. | 15mn | Paperboard  Marqueurs |  |  |  |

A close up of a map

Description automatically generated