MOBILE MONEY

1
2
3
4
5
6

Module 2

Sécurité et prévention

Cofinancé par l'Union européenne

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenus responsables. Numéro de projet : 2023-1-RO01-KA220-ADU-000157797

Partenaires

Asociatia Four Change, Roumanie

Zavod IZRIIS, Slovénie

E-SENIORS : INITIATION DES SENIORS AUXNTIC ASSOCIATION, France

GUnet, Grèce

Asociatia Niciodata Singur - Prietenii Varstnicilor, Roumanie

Fundació Gesmed Fundació de la Comunitat Valenciana, Espagne

Cofinancé par l'Union européenne

MOBILE MONEY

Modules

1. Compétences numériques de base
2. **Sécurité et prévention**
3. Gestion d'un compte bancaire en ligne
4.. Solutions en ligne pour recevoir et envoyer de l'argent
5. Utilisation d'une carte de crédit pour acheter des biens et des services en ligne
6. Traitement des paiements en ligne pour les taxes et les factures

Cofinancé par l'Union européenne

Unité 1

Introduction

Objectifs

À l'issue de cette unité, vous connaitrez:

✓Les objectifs d'apprentissage et le contenu de formation de ce module

✓La méthodologie de formation utilisée et la durée de ce module

Image par vectorjuice sur Freepik

Cofinancé par l'Union européenne

MOBILE MONEY

Compétences

Après avoir suivi ce module, vous pourrez

- Acquérir les compétences nécessaires pour utiliser les solutions de paiements mobiles en toute sécurité et en toute confiance :
  - ✓ Comprendre ce qu'est la sécurité en ligne.
  - ✓ Comprendre ce que sont les données personnelles et sensibles.
  - ✓ Comprendre les concepts de vie privée et de sécurité.
  - ✓ Savoir ce que sont le spamming et le phishing (hameçonnage) et comment y répondre
  - ✓ Connaître les critères permettant de décider quels liens peuvent être visités en toute sécurité
  - ✓ Connaître vos droits en ligne
  - ✓ Comprendre ce qu'est le GDPR et pourquoi nous en avons besoin
  - ✓ Savoir appliquer les mesures de sécurité et de prévention

Cofinancé par l'Union européenne

MOBILE MONEY

Contenu de la formation

1. Introduction de la session : durée, objectifs, contenu et méthodologie
2. Sécurité en ligne, données personnelles, données sensibles, vie privée et sécurité
3. Reconnaître le spam et le phishing et savoir comment y remédier
4. Connaître vos droits en ligne, l'exemple du GDPR
5. Se protéger en ligne
6. Quiz : vérifiez vos connaissances

Cofinancé par l'Union européenne

MOBILE MONEY

Méthodologie et durée de la formation

Durée de la visite : 4 heures

- Session en face à face : 2 heures
- Formation en ligne : 2 heures

Méthodologie

- Active et participative
- Formation en face à face :
  - ✓Dialogue ✓ Travail d'équipe
- Formation en ligne :
  - ✓Mise en œuvre pratique de certains conseils
  - ✓Echange avec les autres participants.

Cofinancé par l'Union européenne

Unité 2

Sécurité en ligne et données personnelles

Objectifs

À l'issue de cette unité, vous saurez :

✓Qu'est-ce que la sécurité en ligne ?

✓Qu'est-ce qu'une donnée à caractère personnel ?

Cofinancé par l'Union européenne

Sécurité en ligne

Le fait de naviguer en ligne expose les utilisateurs d'Internet à des **menaces de sécurité**. Une fois qu'un utilisateur envoie des données sur l'internet (paquets d'appels vidéo ou vocaux, chat, courrier électronique ou numéros de carte de crédit, sites web), il **n'a aucun contrôle sur les personnes qui peuvent accéder à ces données**. Les données passent par de nombreux serveurs, routeurs et appareils où n'importe quel pirate informatique, fournisseur de services ou agent gouvernemental peut y accéder et les lire.

Il est donc de la plus haute importance que les utilisateurs d'Internet prennent des mesures pour :

- Protéger **leurs données personnelles sensibles ;**
- Utiliser des outils et des services en ligne, tels que le cryptage des données, qui **garantissent la confidentialité et la sécurité** des informations des usagers lorsqu'ils communiquent avec eux en ligne.

Qu'est-ce que les données à caractère personnel ?

Les données à caractère personnel sont toutes les informations relatives à une **personne vivante, identifiée ou identifiable**.

Les différents éléments d'information qui, ensemble, peuvent être utilisés pour **identifier une personne spécifique**, sont également des données à caractère personnel.

Image par storyset sur Freepik

Exemples de données à caractère personnel

Voici quelques exemples de données à caractère personnel :

- Nom et prénom ;
- Adresse personnelle ;
- Adresse électronique telle que

  prénom.nom@fournisseur.com ;
- les données de localisation, telles que la fonction de données de localisation d'un téléphone portable) ;
- Numéro de la carte d'identité ;
- Adresse de protocole Internet (IP) ;
- Un identifiant de cookie ;
- L'identifiant publicitaire de votre téléphone ;
- Données détenues par un hôpital ou un médecin, permettant d'identifier une personne de manière unique.

Unité 3

Données sensibles, vie privée et sécurité

Objectifs

Cette unite vise à clarifier :

- ✓ Quelles sont les données personnelles considérées comme sensibles ?
- ✓ Quelle est la différence entre protection de la vie privée et sécurité
- ✓ Qu'est-ce que la protection de la vie privée en ligne et comment assurer la sécurité en ligne ?

Image par vectorjuice sur Freepik

Cofinancé par l'Union européenne

Quelles sont les données personnelles considérées comme sensibles ?

Les données à caractère personnel suivantes sont considérées comme "**sensibles**" et sont soumises à des conditions de traitement spécifiques :

- Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques ;
- Photos, vidéos ;
- Adhésion à un syndicat ;
- Données génétiques, données biométriques traitées uniquement à des fins d'identification d'un être humain ;
- Données relatives à la santé ;
- Données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne.

Données financières sensibles

- Compte et mot de passe d’un système de banque en ligne
- Le CCV, la date d'expiration d'une carte de crédit ou de débit
- Le code PIN de votre téléphone portable

Image par redgreystock sur Freepik

Qu’est-ce qu’un cookie?

- Un cookie, c’est un petit fichier que votre ordinateur ou votre téléphone reçoit quand vous visitez un site internet.
- Il aide le site à se souvenir de vous, par exemple pour ne pas vous redemander votre mot de passe ou pour garder vos articles dans un panier d’achat.
- Certains cookies sont utiles (comme garder votre langue préférée).
- D’autres cookies suivent vos habitudes pour vous montrer des publicités ou vendre vos informations à d’autres entreprises.

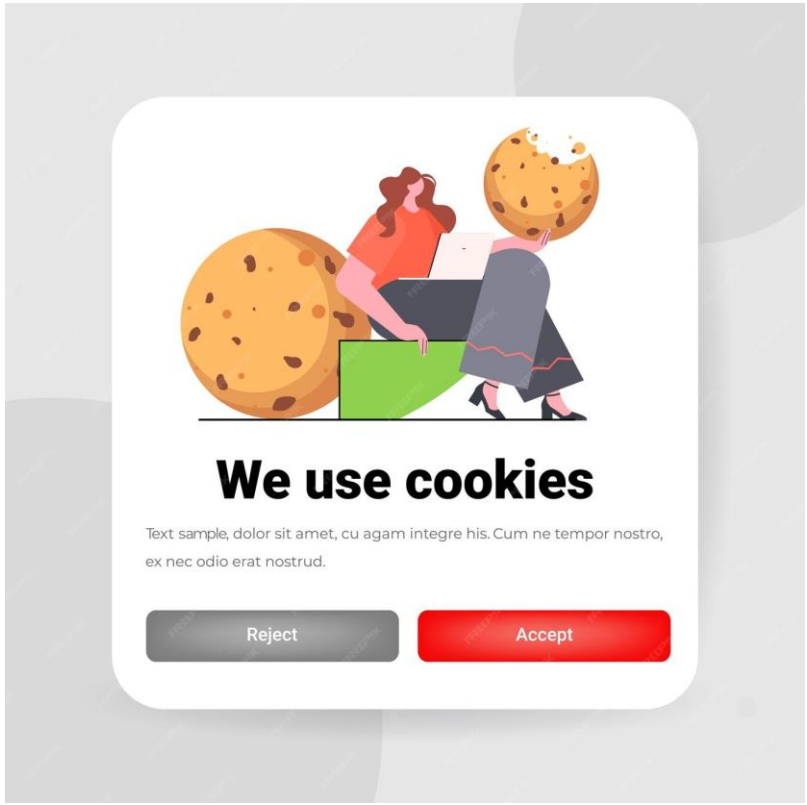

Image par redgreystock sur Freepik

Qu'est-ce que la vie privée ?

La protection de la vie privée, c'est:

- Comment nous **contrôlons nos données personnelles,** et
- **l'utilisation qui en est faite** par les tiers qui les ont reçues, de manière sécurisée.

Pensez aux **politiques de confidentialité que** l'on vous demande de lire et d'accepter lorsque vous visitez un site web ou téléchargez une nouvelle application pour smartphone.

Image par Freepik

Qu'est-ce que la sécurité ?

La sécurité consiste **à protéger vos données personnelles** contre tout **accès non autorisé,** que ce soit sur votre appareil, sur le serveur web distant ou lors d'une communication sur l'internet.

Nous utilisons des **contrôles de sécurité** au niveau technique pour limiter l'accès aux informations. Ces contrôles sont en place :

- Sur nos appareils (PC, tablette, téléphone portable), c'est-à-dire en appliquant les mises à jour du système d'exploitation et des logiciels, en utilisant des mots de passe forts ;
- Sur le serveur web, en utilisant des mots de passe forts ;
- Lors de la transmission d'informations sur l'internet, en utilisant le protocole sécurisé **https.**

Image by vectorjuice on Freepik

Sécurité et protection de la vie privée

- La sécurité concerne la **protection des données**, tandis que la **protection de la vie privée** concerne la **protection de l'identité des utilisateurs**.

  Par exemple, le personnel des hôpitaux et des cliniques utilise des systèmes sécurisés pour communiquer avec les patients au sujet de leur santé, plutôt que d'envoyer des informations via des comptes mails personnels. Ce type de communication est un exemple de sécurité.

- D'autre part, la politique et les dispositions en matière de protection de la vie privée peuvent limiter l'accès aux dossiers médicaux des patients à **certains membres du personnel de l'hôpital**, tels que les médecins, les infirmières et les assistants médicaux.

- **Il est possible d'avoir la sécurité sans la protection de la vie privée**.

  En effet, par exemple, des données personnelles peuvent être transmises et stockées sur un site web en toute sécurité, mais le site web peut toujours les vendre.

- **Il n'est pas possible d'avoir la protection de la vie privée sans sécurité.**

  En effet, par exemple, un pirate informatique pourrait obtenir un accès non autorisé à votre appareil, à votre serveur web ou aux données transmises et voler vos données personnelles.

Unité 3

Spam et hameçonnage

Objectifs

À l'issue de la formation, vous saurez :

- ✓ Qu'est-ce que le spam et le phishing (hameçonnage) ?
- ✓ Comment identifier le spam
- ✓ Quand un lien peut être consulté en toute sécurité

Cofinancé par l'Union européenne

Qu'est-ce que le spam et le hameçonnage ?

Vous avez peut-être reçu des courriels malvenus d'un **expéditeur inconnu**, généralement de nature commerciale.

En outre, les **courriels** peuvent être **dangereux** car ils peuvent contenir des liens menant à des sites web de **hameçonnage/phishing** (collecte illégale de données) ou à des sites web hébergeant des logiciels malveillants ou contenant des logiciels malveillants en pièce jointe.

N'ouvrez donc **aucun fichier joint et ne cliquez sur aucun lien**. Ne communiquez jamais vos données personnelles, les détails de votre compte bancaire en ligne (nom d'utilisateur, mot de passe) ou les détails de votre carte de crédit/débit, tels que la date d'expiration et les 3 chiffres du code CCV.

Ce qu'on appelle l'**hameçonnage** est le procédé par lesquels les criminels envoient des courriels d'apparence officielle pour vous inciter à révéler des informations susceptibles d'être utilisées pour le vol d'identité.

Comment identifier le spam ?

Un courriel est suspect s'il contient un ou plusieurs des éléments suivants

- Erreurs de grammaire et d'orthographe
- Courriers en langue étrangère
- Le nom de l'expéditeur est manquant
- Nécessité urgente d'agir - en particulier en cas de menace

- Invitation à saisir des données personnelles (par exemple, PIN)
- Demande d'ouverture d'un fichier
- Une banque ou un fournisseur qui n’est pas le vôtre ou qui ne vous a jamais écrit.

Image par freepik

Que faire ou ne pas faire ?

- ✓ N'ouvrez pas les pièces jointes si elles n'ont pas été analysées par un programme antivirus.
- ✓ N'oubliez pas de vous déconnecter, surtout si vous utilisez un ordinateur public partagé.
- ✓ Supprimez tous les courriels provenant de personnes inconnues.
- ✓ Ne répondez jamais aux spams !
- ✓ Ne cliquez pas sur les liens contenus dans les courriers électroniques non sollicités.

Activité : Le lien est-il sûr ?

Décidez si le lien peut être consulté en toute sécurité :

Supposons que vous receviez un courriel d'une banque vous demandant de cliquer sur un lien comme celui ci-dessous et de soumettre des données personnelles, telles que votre nom d'utilisateur, vos mots de passe et les détails de votre carte de crédit.

http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asDvdva

1. *Ne vous précipitez pas, réfléchissez-y et décidez si vous pouvez visiter ce lien en toute sécurité.*
2. *Expliquez votre décision.*

Activité : Le lien est-il sûr ? (2)

La réponse. *Ce lien* **n'est pas sécurisé** pour plusieurs raisons :

- Il utilise http au lieu de https.
- Le nom de domaine n'est pas lié au nom officiel de la banque.
- Le lien est étrangement long.
- Le nom de domaine du lien est différent du nom de domaine de l'adresse électronique de l'expéditeur.
- Une vraie banque ne demandera jamais de noms d'utilisateur, de mots de passe ou d'informations sur les cartes de crédit.

Unité 4

Quels sont vos droits en ligne ?

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Quels sont vos droits et obligations en ligne ?
- ✓ Qu'est-ce que le GDPR et pourquoi en avons-nous besoin ?

Cofinancé par l'Union européenne

Nous sommes des citoyens numériques

Les citoyens numériques peuvent jouir des droits à la vie privée, à la sécurité, à l'accès et à l'inclusion, à la liberté d'expression, etc.
Toutefois, ces droits s'accompagnent de certaines responsabilités, telles que l'éthique et l'empathie, ainsi que d'autres responsabilités visant à garantir un environnement numérique sûr et responsable pour tous.

Nous sommes désormais tous reliés par l'internet, comme les neurones d'un cerveau géant.

Stephen Hawking

Qu'est-ce que le RGPD et qui doit s'y conformer ?

Qu'est-ce que le RGPD ?

- Le **règlement général sur la protection des données** est une loi de l'Union européenne qui a été mise en œuvre le 25 mai 2018 et qui oblige les organisations à protéger les données personnelles et à faire respecter le droit à la vie privée de toute personne se trouvant sur le territoire de l'UE.

Qui doit se conformer au RGPD ?

- Toute organisation qui traite des données personnelles d'individus dans l'UE doit se conformer au RGPD.
- Le terme "**traitement**" est un terme large qui couvre à peu près tout ce que l'on peut faire avec des données : collecte, stockage, transmission, analyse, etc.
- Les "**données à caractère personnel**" sont toutes les informations relatives à une personne, telles que le nom, l'adresse électronique, l'adresse IP, la couleur des yeux, les convictions politiques, etc.

Conformité

Même si une organisation n'a aucun lien avec l'UE elle-même mais traite des données personnelles de personnes dans l'UE (par exemple, par le biais d'un suivi sur son site web), elle doit toujours se conformer au RGPD.

Le RGPD ne se limite pas aux entreprises à but lucratif.

Les bienfaits du RGPD

- Le RGPD est là pour protéger vos droits en tant qu'utilisateur.
- Il est bon de savoir à quoi vous consentez quand vous utilisez un site.
- Bien gérer les usagers vulnérables n'est pas seulement une attente de la loi, c'est aussi la bonne chose à faire sur le plan social et une décision commerciale intelligente.
- Les sites doivent vous expliquer clairement à quoi servent les cookies (voir diapositive 15) , vous demander votre accord pour les utiliser et vous pouvez tout à fait refuser.

Unité 5

Comment se protéger à l'avance

Objectifs

À l'issue de cette unité, vous saurez :

✓ Comment vous protéger en identifiant les sites sûrs, les liens et les demandes de consentement.

Image by vectorjuice on Freepik

Cofinancé par l'Union européenne

Quelques conseils pour votre sécurité (1/3)

- Évitez de payer qui que ce soit par virement bancaire, Western Union, mandat ou carte-cadeau. Les escrocs demandent souvent ce type de paiement car il ne laisse pas de trace écrite.
- Ne communiquez jamais vos mots de passe à quiconque en ligne. Ne les communiquez qu'à une personne de confiance, comme un membre de votre famille.
- Soyez sceptique face à tout ce qui est urgent. Les escrocs veulent souvent que vous agissiez avant d'avoir le temps de réfléchir à la situation. N'oubliez pas de prendre du recul et de vous éloigner de l'ordinateur au lieu de paniquer si vous pensez que quelque chose est suspect et que vous n'êtes pas sûr de la marche à suivre.
- Cliquez immédiatement sur le X ou le Non pour fermer les sites web ou les fenêtres pop-up suspects (ex: vous avez gagné à la loterie!).

Quelques conseils pour votre sécurité (2/3)

- Appelez un proche ou cherchez des conseils en ligne
- Consultez Google pour voir si d'autres personnes ont signalé de telles escroqueries.
- Veillez à ce que les sites web soient précédés de la mention https://. Le "**s**" indique que le site est sécurisé. Le nom doit également être accompagné d'un petit cadenas.
- Méfiez-vous de tout ce qui semble trop beau pour être vrai.
- Pensez à activer l'authentification multifactorielle. Celle-ci vous oblige à saisir un code (envoyé par SMS ou par courriel) ou à utiliser une application pour vous connecter à certains de vos comptes, y compris les réseaux sociaux ou les comptes bancaires en ligne. Cela peut empêcher les pirates d'avoir accès à vos comptes et données.

Quelques conseils pour votre sécurité (3/3)

- Des précautions supplémentaires peuvent être prises pour éviter les escroqueries.
- Personne ne doit craindre de continuer à utiliser l'internet, à condition de savoir comment l'utiliser en toute sécurité.
- Trouvez un espace sûr au sein de votre communauté ou de votre cercle social où vous pouvez vous sentir à l'aise pour discuter de ces questions sans craindre d'être jugé.

Si une escroquerie a déjà eu lieu, voici quelques mesures à prendre :

- Appelez votre banque. Elle peut geler votre compte afin que personne ne puisse accéder à vos fonds et vous délivrer une nouvelle carte de débit. Si de l'argent a déjà été volé, vous pouvez demander à la banque d'annuler ces transactions et de vous restituer vos fonds.
- Envisagez de porter plainte auprès de la police.

MOBILE MONEY

Vérifiez vos connaissances !

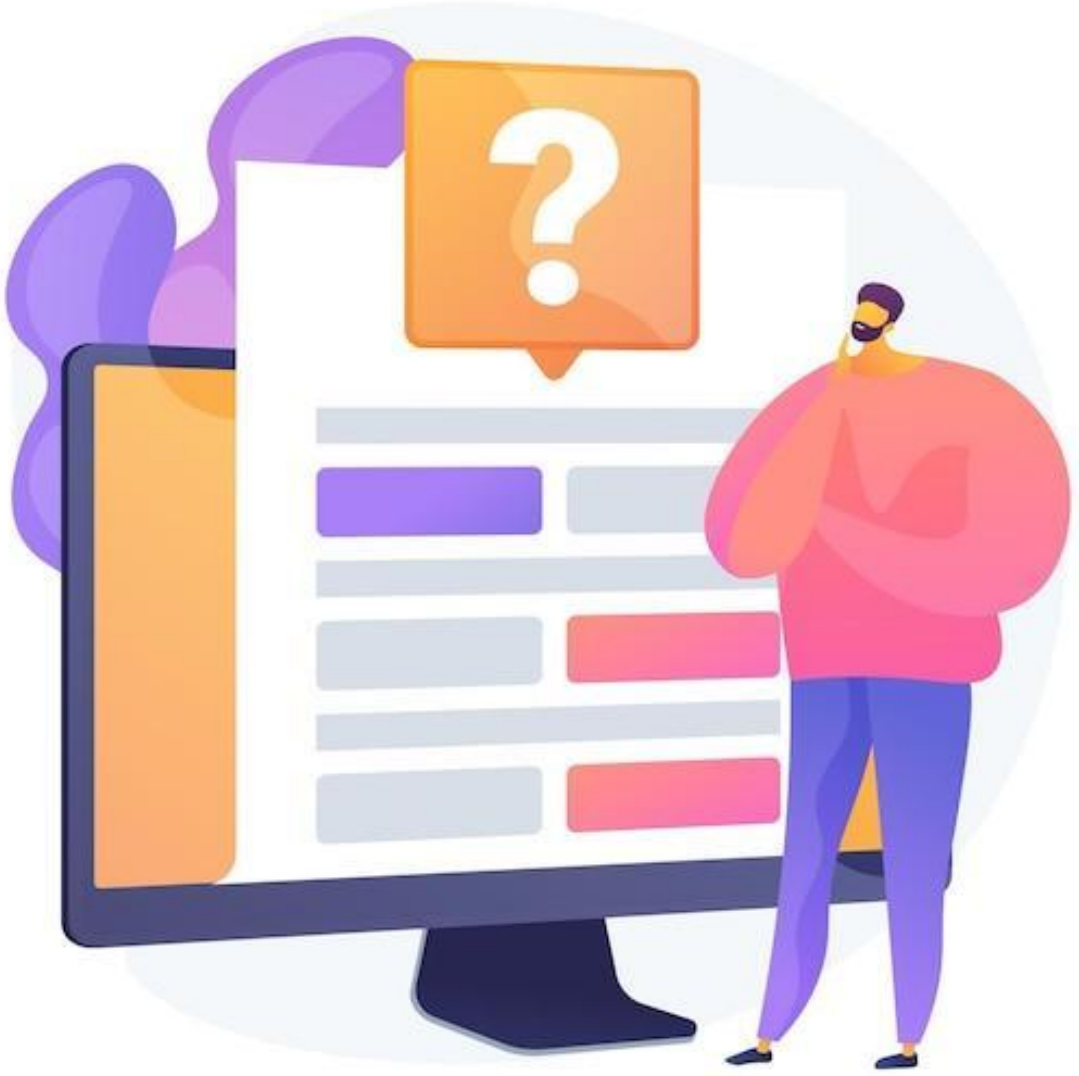

Image by vectorjuice on Freepik

1. Lequel des mots de passe suivants est le plus fort ?

Une seule réponse est correcte !

A. John1234

B. John1990

C. John051190

D. J0Hn!2nO

2. Parmi les éléments suivants, lesquels sont des données à caractère personnel ?

Une seule réponse est correcte !

A. Adresse IP

B. Adresse électronique

C. Tous

D. Cookies dans un navigateur

3. Lorsque le symbole du cadenas apparaît dans le navigateur, cela signifie que le navigateur a verrouillé la page parce qu'elle n'est pas sécurisée.

Oui, c’est vrai

Non, c’est faux

4. Lequel des éléments suivants n'est PAS une donnée personnelle sensible ?

Une seule réponse est correcte !

A. Photos

B. Adresse du domicile

C. Données relatives à la santé

D. Opinions politiques

5. L'expéditeur peut-il être un indicateur du caractère indésirable d'un courrier électronique ?

Qui

Non

6. Que ne devez-vous jamais faire si vous recevez un prétendu courrier indésirable ?

Une seule réponse est correcte !

A. Supprimer l'e-mail

B. Vérifier l'émetteur

C. Vérifier le sujet

D. Répondre et demander s'il s'agit d'un spam

MOBILE MONEY

Félicitations !

Vous avez terminé ce module !

Cofinancé par l'Union européenne

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenus responsables. Numéro de projet : 2023-1-RO01-KA220-ADU-000157791