



MOBILE MONEY

Module 4

Recevoir et envoyer de l'argent en ligne



**Cofinancé par
l'Union européenne**

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive « Éducation, audiovisuel et 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



ZAVOD IZRIIS

Zavod IZRIIS, Slovénie



Asociația Four Change, Roumanie



E-SENIORS: INITIATION DES
SENIORS AUX NTIC
ASSOCIATION, France



GREEK UNIVERSITIES NETWORK

GUnet, Grèce



NICIODATĂ SINGUR
prietenii vârstnicilor

Asociația 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 & Prévention

3. Gestion d'un compte bancaire en ligne

4. Recevoir et envoyer de l'argent en ligne

5. Utilisation d'une carte de crédit pour l'achat de biens et de services en ligne

6. Traitement des paiements en ligne pour les taxes et les factures

Unité 1

Introduction

Objectifs

À la fin de cette unité, vous en saurez plus sur

- ✓ Les objectifs d'apprentissage et le contenu de formation de ce module
- ✓ La méthodologie de formation utilisée et la durée de ce module





Compétences

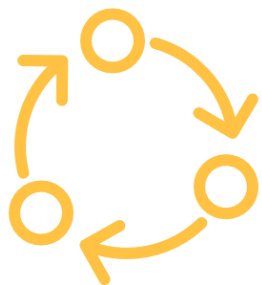
Après avoir suivi ce module, vous pourrez :

- Comprendre et effectuer des transactions numériques
 - ✓ Identifier les informations nécessaires pour envoyer de l'argent.
 - ✓ Savoir ce que signifie IBAN et comment l'utiliser.
 - ✓ Comprendre l'utilité d'un nom d'utilisateur.
 - ✓ Savoir quand et pourquoi utiliser les numéros de téléphone.
 - ✓ Ajoutez des détails de paiement clairs.
- Franchir les étapes de sécurité en toute confiance
 - ✓ Comprendre comment les codes PIN protègent votre compte.
 - ✓ Utiliser les mots de passe de manière efficace et sûre.
 - ✓ Reconnaître le niveau de sécurité supplémentaire offert par les codes SMS.
 - ✓ Évitez de partager des détails sensibles avec d'autres personnes.
 - ✓ Identifier les signes de connexions sécurisées (par exemple les icônes de cadenas).



Contenu de la formation

1. Introduction aux transferts numériques de fonds : aperçu des compétences numériques de base nécessaires pour les transferts d'argent par téléphone portable.
2. Comprendre les formulaires et les champs de données obligatoires : IBAN, nom d'utilisateur, numéro de téléphone et détails de paiement dans les formulaires.
3. Applications pour envoyer et recevoir de l'argent : Présentation des applications couramment utilisées pour les transferts d'argent, de leurs fonctionnalités et de la manière de les installer.
4. Identifier et éviter les escroqueries courantes : Reconnaître les tentatives d'hameçonnage et gérer en toute sécurité les données personnelles pour prévenir la fraude.
5. Accéder à l'historique des transactions et le comprendre : consulter les paiements antérieurs, les détails de l'expéditeur et tenir des registres à l'aide d'applications mobiles.
6. Conseils et exercices pratiques



Méthodologie et durée de la formation

Durée : 4 heures

- Formation en présentiel : 2 heures
- Formation en ligne : 2 heures

Méthodologie

- Active et participative
- Formation en présentiel :
 - ✓ Dialogue
 - ✓ Jeu de rôle
 - ✓ Travail d'équipe
- Formation en ligne :
 - ✓ Vidéos sélectionnées ou autoproduites
 - ✓ Mise en pratique de quelques conseils donnés en classe
 - ✓ Quelques travaux en collaboration
 - ✓ Simulation

Unité 2

Introduction aux transferts numériques de fonds

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Comprendre le rôle des transferts numériques de fonds
- ✓ Identifier les compétences numériques de base
- ✓ Reconnaître l'importance des outils numériques
- ✓ Instaurer la confiance dans l'utilisation de la technologie



Qu'est-ce que le transfert numérique de fonds ?

Le transfert numérique de fonds est **un moyen d'envoyer ou de recevoir de l'argent par voie électronique à l'aide d'applications mobiles ou de plateformes en ligne, sans avoir besoin d'espèces ou de chèques.**

Comment ça marche : vous fournissez des informations telles que l'IBAN ou le nom d'utilisateur du destinataire, et l'argent est transféré en toute sécurité via votre banque ou votre application.



Rôle du transfert numérique de fonds

Les transferts numériques de fonds révolutionnent la façon dont les individus gèrent leurs finances en offrant des solutions sûres, efficaces et rapides pour envoyer et recevoir de l'argent. Ils remplacent le besoin d'argent liquide, réduisent les risques de vol ou de perte et permettent aux utilisateurs d'effectuer des transactions depuis le confort de leur foyer. De plus, ils fournissent des enregistrements détaillés pour chaque transaction, ce qui facilite le suivi et la vérification de la responsabilité financière.

Principaux avantages des transferts numériques de fonds :

- **Praticité** : Effectuez des transactions à tout moment et en tout lieu.
- **Rapidité** : Transferts d'argent immédiats ou quasi-instantanés entre comptes.
- **Sécurité** : L'authentification en plusieurs étapes et le cryptage protègent les fonds.
- **Tenue d'archives** : Accédez à l'historique détaillé des transactions pour une meilleure gestion financière.
- **Rentabilité** : frais moins élevés que les méthodes traditionnelles telles que les traites bancaires ou les mandats.



Exemples de transferts numériques de fonds

- Envoi d'argent à la famille ou aux amis
- Paiement des services
- Bénéficiaire d'une pension ou d'une aide financière
- Achats en ligne
- Partager les factures avec des amis
- Faire un don à une cause



Compétences de base nécessaires pour les transferts numériques de fonds (1/2)

1. **Utiliser un appareil mobile ou d'un ordinateur** : savoir utiliser un smartphone, une tablette ou un ordinateur pour accéder à des applications ou à des sites Web.
2. **Remplir les formulaires** : saisissez avec précision les informations requises telles que l'IBAN, le nom du destinataire et le montant du paiement.
3. **Naviguer dans les applications ou les sites web** : apprenez à ouvrir, à vous connecter et à explorer les applications de transfert d'argent ou les sites web bancaires.



Compétences de base nécessaires pour les transferts numériques de fonds (2/2)

4. **Comprendre les mesures de sécurité** : utilisez des codes PIN, des mots de passe et des codes SMS pour sécuriser vos transactions.
5. **Vérifier l'historique des transactions** : localisez et examinez les transactions passées pour confirmer les paiements ou les reçus.
6. **Communiquer clairement les informations** : fournissez et demandez des informations précises, telles que l'IBAN ou les références de la transaction, afin d'éviter les erreurs.



Les potentiels problèmes qui peuvent survenir lors des transferts numériques

- Saisie d'informations erronées
- Escroqueries et hameçonnage
- Habitudes inadaptées en matière de sécurité
- Problèmes de connectivité
- Utilisation d'applications ou de logiciels obsolètes
- Mauvaise compréhension des frais ou des taux de change



Unité 3

Comprendre les formulaires et les données obligatoires

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Identifier les champs de données clés
- ✓ Surveiller avec votre précision vos données
- ✓ Reconnaître les champs obligatoires et ceux facultatifs
- ✓ Vérifier les informations fournies par d'autres personnes



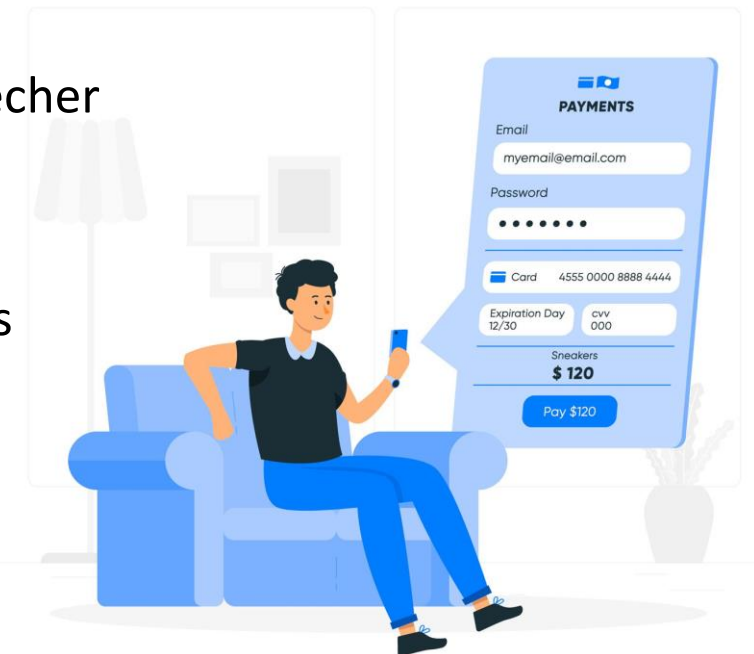
Champs de données clés

- **IBAN (International Bank Account Number)**
 - Un code unique qui identifie le compte bancaire du destinataire.
 - Essentiel pour s'assurer que l'argent arrive à la bonne destination.
- **Nom d'utilisateur ou Nom**
 - Le nom ou le nom d'utilisateur de l'application de la personne recevant l'argent.
 - Aide à confirmer l'identité du destinataire.
- **Numéro de téléphone**
 - Utilisé pour certaines applications de paiement ou comme étape de vérification supplémentaire.
 - Garantit des transactions sécurisées et précises.
- **Informations de paiement**
 - Une courte note décrivant l'objet du transfert (par exemple, « Cadeau pour mon petit-fils »).
 - Aide l'expéditeur et le destinataire à garder une trace de la transaction.



Conseils pour garantir l'exactitude des transferts numériques de fonds (1/2)

- **Ne pas utiliser de réseau Wi-Fi public**
 - Utilisez des réseaux sécurisés ou des données mobiles pour empêcher tout accès non autorisé à vos informations.
- **Vérification supplémentaire de toutes les informations**
 - Vérifiez l'IBAN, le nom d'utilisateur, le numéro de téléphone et les détails du paiement.
 - Même une petite faute de frappe peut envoyer de l'argent sur le mauvais compte.
- **Vérification par recoupement avec le destinataire**
 - Demandez au destinataire de confirmer les détails, en particulier pour les nouvelles transactions.
 - Enregistrez les informations vérifiées pour une utilisation future en toute sécurité.



Conseils pour garantir l'exactitude des transferts numériques de fonds (2/2)

■ Prenez votre temps

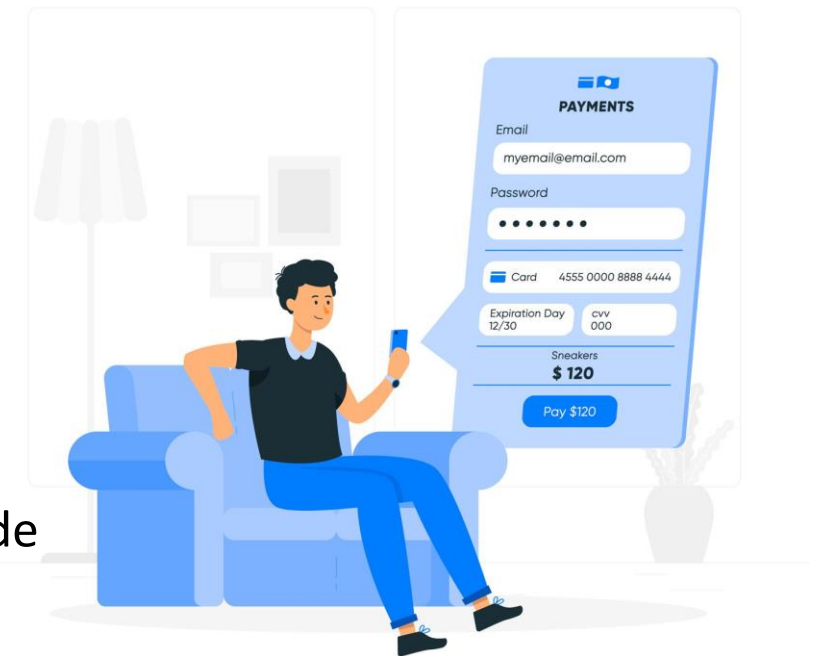
- Évitez de vous précipiter lorsque vous saisissez des détails.
- Une approche calme réduit le risque d'erreurs.

■ Utilisez le remplissage automatique avec précaution

- Vérifiez que les informations enregistrées sont correctes avant d'utiliser les fonctions de saisie automatique.
- Mettez à jour les informations obsolètes de votre application ou de votre compte.

■ Examinez l'écran de confirmation

- Vérifiez le récapitulatif final de la transaction avant de la soumettre.
- Faites attention au nom du destinataire et au montant à envoyer.



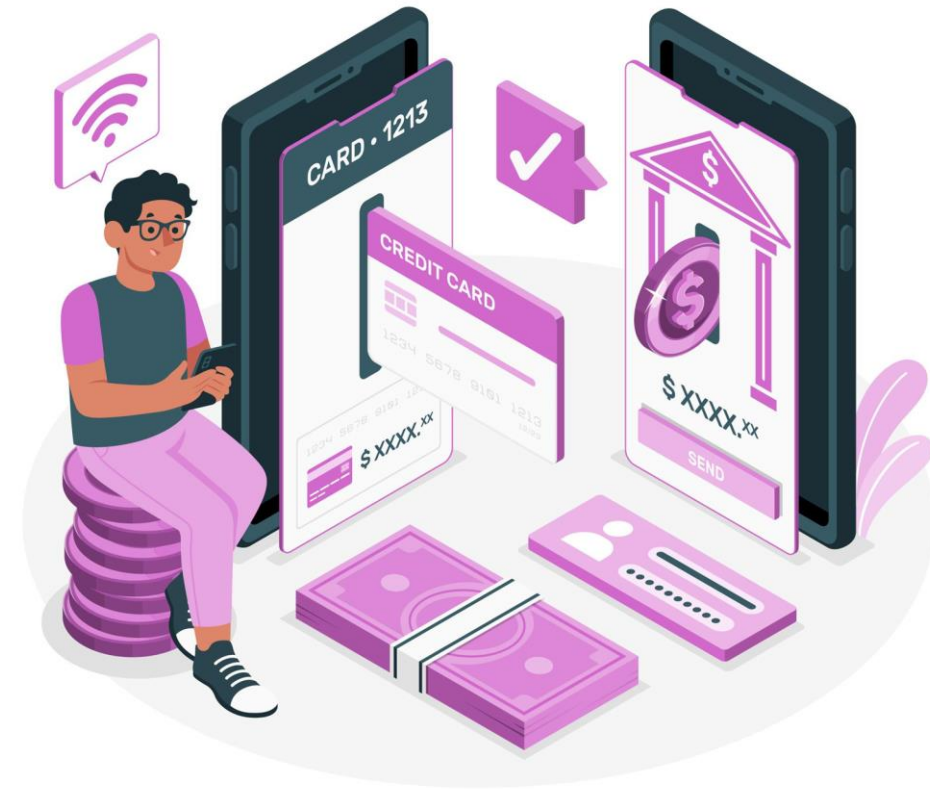
Unité 4

Applications pour envoyer et recevoir de l'argent

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Reconnaître les applications couramment utilisées
- ✓ Comprendre les fonctionnalités des applications
- ✓ Installer et configurer les applications
- ✓ Comparer les options des applications



Applications couramment utilisées pour envoyer et recevoir de l'argent en France

- **Lydia** – Application créée par une start-up française et désormais l'une des plus utilisée en France, Lydia permet de payer, transférer de l'argent sur son compte bancaire et créer des cagnottes en ligne.
- **Revolut** - Application financière mondiale populaire en France, Revolut fournit des services tels que des transferts internationaux, des opérations de change et des outils de budgétisation, avec plus de 16 millions d'utilisateurs dans le monde.
- **PayPal** - Une plateforme mondialement reconnue pour les paiements et les transferts d'argent en ligne. De nombreux Français utilisent PayPal pour faire des achats en ligne et recevoir des paiements de l'étranger.
- **Western Union** - Offre des services de transfert d'argent en ligne et en agence. Western Union est une entreprise de confiance en France pour l'envoi et la réception de fonds, en particulier de sources internationales.



Installer et configurer les applications de transfert d'argent

- **Choisissez la bonne application** : identifiez l'application qui correspond à vos besoins (par exemple, Revolut ou PayPal, ou l'application de votre banque).
- **Téléchargez l'application** : rendez-vous sur l'App Store (iPhone) ou sur Google Play Store (Android). Recherchez l'application par son nom et cliquez sur « Installer ».
- **Créez un compte** : ouvrez l'application et suivez la procédure d'inscription. Fournissez des informations telles que votre nom, votre e-mail, votre numéro de téléphone, un mot de passe sécurisé ou d'autres informations fournies par la banque. En général, pour créer un compte bancaire en ligne, vous devez d'abord vous rendre à la banque.
- **Associez votre compte bancaire ou votre carte** : pour certaines applications, saisissez votre IBAN ou votre numéro de carte en toute sécurité. Suivez les étapes de vérification requises (par exemple, code par SMS ou e-mail).
- **Configurez les fonctions de sécurité** : activez le code PIN, le mot de passe ou l'authentification biométrique (reconnaissance des empreintes digitales/visage). Activez l'authentification à deux facteurs pour une protection supplémentaire.
- **Entraînez-vous à naviguer dans l'application** : explorez l'interface pour trouver des fonctionnalités telles que l'envoi d'argent, la consultation des transactions et la mise à jour des détails. Familiarisez-vous avec les options d'aide ou d'assistance en cas de problème.



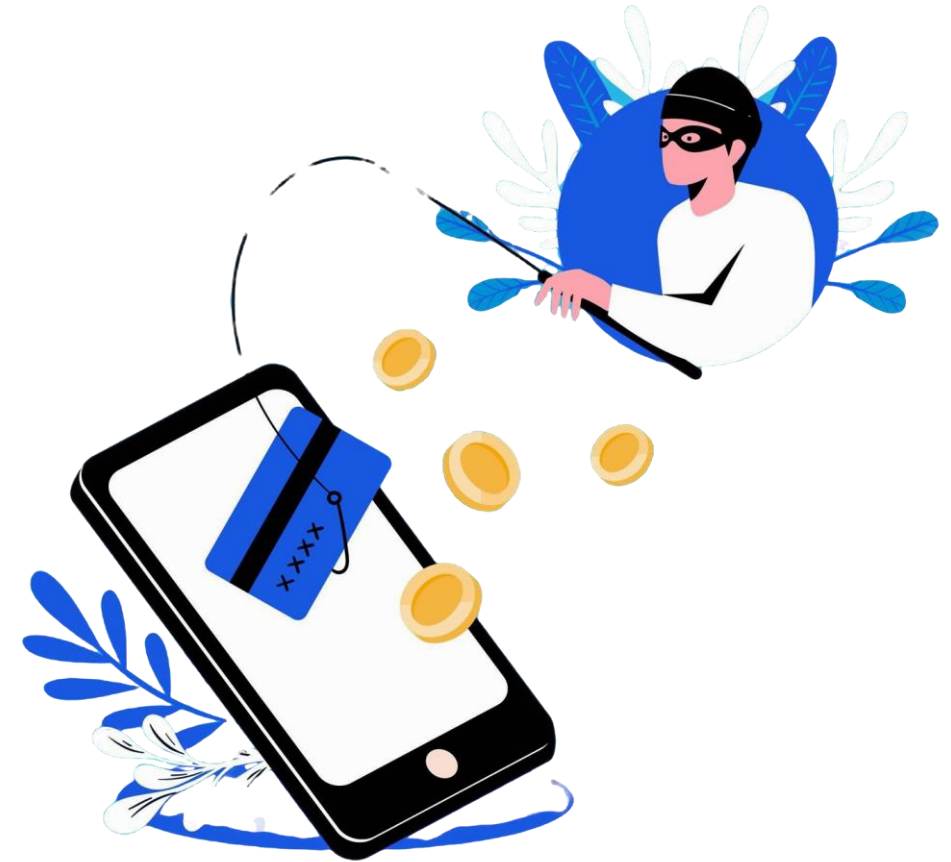
Unité 5

Identifier et éviter les arnaques courantes

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Reconnaître les tentatives d'hameçonnage
- ✓ Comprendre les pratiques de partage sécurisé
- ✓ Vérifier les demandes ou offres légitimes
- ✓ Identifier les canaux de communication sécurisés



Que sont les tentatives d'hameçonnage ?

Le phishing (hameçonnage) est une escroquerie par laquelle des pirates tentent de vous inciter à partager des informations personnelles ou financières par le biais de faux messages, e-mails ou sites Web.

- **Comment cela fonctionne :**
 - Les escrocs se font passer pour des institutions de confiance (banques, agences gouvernementales ou prestataires de services).
 - Ils envoient des messages vous demandant de cliquer sur un lien, de fournir des informations de connexion ou de confirmer une transaction.

- **Signes courants d'hameçonnage**

- Langage alarmiste tel que « Votre compte sera bloqué ! »
- Des adresses e-mail ou des numéros de téléphone inconnus.
- Mauvaise orthographe et grammaire dans le message.
- Demandes d'informations sensibles telles que codes PIN ou mots de passe.
- Liens suspects qui ne correspondent pas au site officiel.

- **Exemples d'hameçonnage**

- De faux e-mails prétendant provenir de votre banque et vous demandant de vérifier votre compte.
- SMS contenant un lien pour « résoudre » un problème avec votre compte.
- Appels prétendant que vous avez gagné un prix et demandant vos informations bancaires.



Pratiques de partage sécurisé

Pour envoyer de l'argent

- Vérifiez les informations du destinataire (par exemple, IBAN, nom d'utilisateur) avant de confirmer.
- Ne partagez que des informations vérifiées et exactes pour éviter les erreurs.
- Évitez de partager des informations sensibles, telles que des mots de passe ou des codes de sécurité, avec d'autres personnes.
- Informez le destinataire une fois le transfert terminé pour s'assurer qu'il est au courant.

Pour recevoir de l'argent

- Fournissez des coordonnées bancaires claires et correctes (par exemple, IBAN ou numéro de téléphone).
- Utilisez des canaux sécurisés (applications de confiance ou communication officielle) pour partager les informations de compte.
- Confirmez la réception des fonds et avertir l'expéditeur en cas d'anomalie.
- Vérifiez les notifications et les rapports de transaction pour s'assurer que les fonds ont été correctement déposés.



Qu'est-ce que l'authentification multifactorielle ?

L'**authentification multifactorielle (MFA)** est une méthode de sécurité qui nécessite deux étapes de vérification ou plus pour confirmer votre identité lors d'une connexion ou d'une transaction.

Fonctionnement de la MFA :

- Première étape :
 - Saisissez votre mot de passe ou votre code PIN.
- Seconde étape :
 - Effectuez une vérification supplémentaire, telle que :
 - Recevoir un code unique par SMS.
 - Utiliser une empreinte digitale ou de la reconnaissance faciale.
 - Générer un code via une application d'authentification.





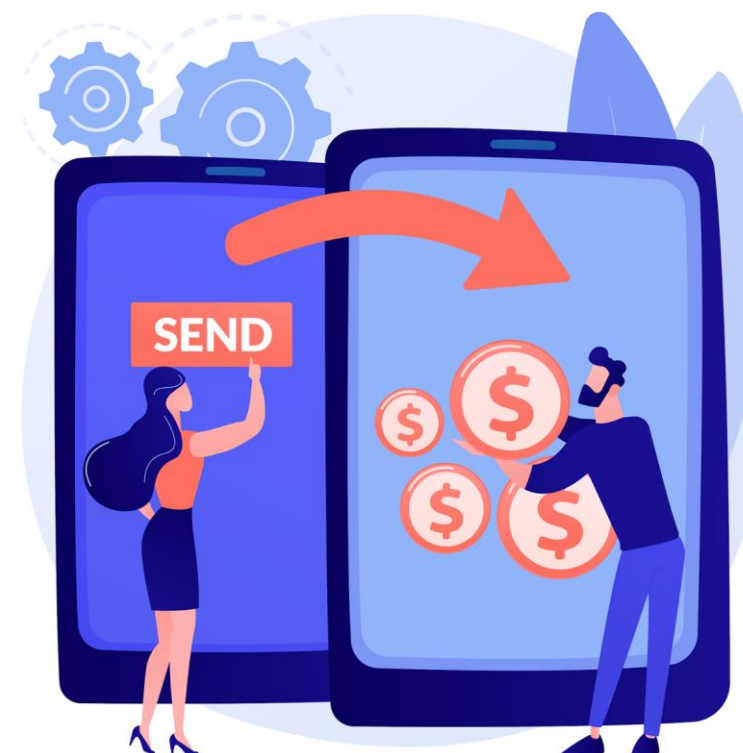
Unité 6

Accéder à l'historique des transactions et le comprendre

Objectifs

À l'issue de cette unité, vous saurez :

- ✓ Naviguer dans l'historique des transactions
- ✓ Comprendre les détails clés d'un rapport de transaction
- ✓ Vérifier les paiements et les reçus
- ✓ Télécharger et gérer les enregistrements



Naviguer dans l'historique des transactions (1/2)

- **Ouvrir l'application ou le site Web**
 - Connectez-vous à votre application bancaire ou à votre plateforme de transfert d'argent à l'aide de vos identifiants.
 - Localisez la section des transactions : Recherchez les onglets ou les menus intitulés « Historique des transactions », « Activité » ou « Paiements ». Ils se trouvent souvent sur l'écran d'accueil ou dans le menu principal.
- **Filtrer votre recherche**
 - Utilisez les filtres disponibles tels que la date, le montant ou le type de transaction pour trouver des enregistrements spécifiques. Par exemple, sélectionnez « Envoyé » ou « Reçu » pour affiner les résultats.



Naviguer dans l'historique des transactions (2/2)

- **Afficher les détails**
 - Cliquez ou tapez sur une transaction pour voir tous les détails, y compris l'expéditeur, le montant et le numéro de référence.
 - Vérifiez que les informations correspondent à vos attentes.
- **Sauvegarder pour une utilisation ultérieure**
 - Si nécessaire, téléchargez ou imprimez les détails de la transaction pour vos dossiers personnels ou comme preuve de paiement.



En quoi est-ce important ?

- **Vérification des transactions**
 - Confirmer que les paiements ont été envoyés ou reçus avec succès
- **Preuve de paiement**
 - Utiliser l'historique des transactions comme preuve des paiements ou des reçus effectués, le cas échéant
- **Suivi financier**
 - Surveiller vos dépenses et vos revenus pour mieux gérer votre budget
- **Résolution des erreurs**
 - Identifier rapidement les anomalies ou les transactions non autorisées pour une résolution rapide.





Activité : Identifiez votre IBAN (1)

Déterminez **la meilleure façon de connaître votre IBAN.**

Vous identifierez les étapes nécessaires pour trouver votre IBAN à l'aide de l'application, du site web ou de relevés de compte imprimés de votre banque.

Partagez les étapes que vous avez suivies avec le groupe pour aider chacun à comprendre les différentes méthodes disponibles.

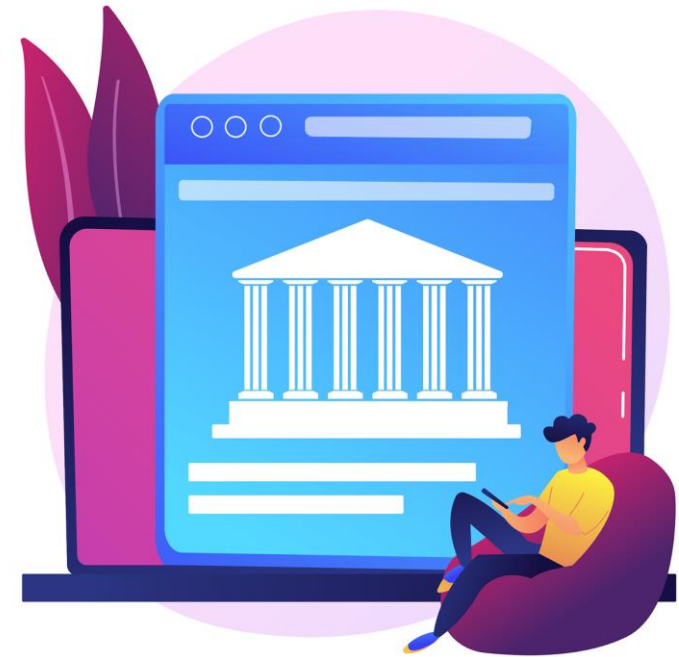




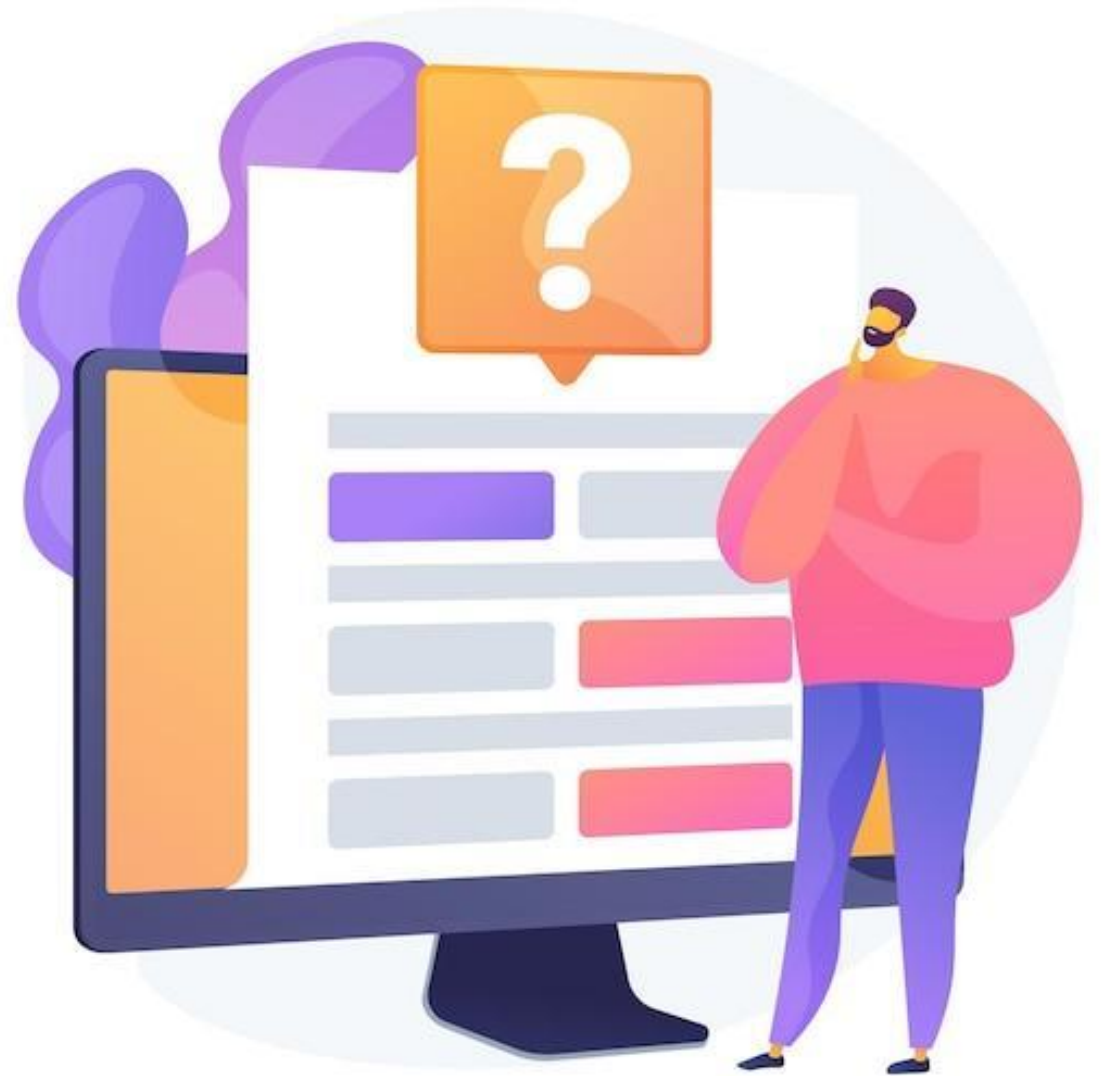
Activité : Identifiez votre IBAN (1)

Questions pour le groupe

- Quels outils ou ressources avez-vous utilisés pour trouver votre IBAN ?
- Avez-vous rencontré des difficultés lors de la localisation de votre IBAN et comment les avez-vous surmontées ?
- Quelles mesures prendriez-vous pour communiquer votre IBAN en toute sécurité si quelqu'un voulait vous envoyer de l'argent ?



Testez vos connaissances !



4 Recevoir et envoyer de l'argent

1. Que faire si vous recevez un e-mail vous demandant les détails de votre compte ?

Une seule réponse est correcte !

A. Répondez immédiatement en indiquant vos coordonnées

B. Cliquez sur le lien dans l'e-mail pour vérifier votre compte

C. Ignorez l'e-mail et le supprimer

D. Partagez votre IBAN en toute sécurité via l'e-mail



2. Lequel des éléments suivants est un exemple de méthode d'authentification multifacteur ?

Une seule réponse est correcte !

A. Utilisation d'un mot de passe uniquement

B. Réception d'un code SMS après avoir saisi votre mot de passe

C. Accès à votre compte sur un réseau Wi-Fi public

D. Connexion sans code confidentiel



3. Que devez-vous faire avant de confirmer un transfert d'argent ?

Une seule réponse est correcte !

A. Faites-le sans attendre

B. Vérifiez à nouveau les coordonnées du destinataire

C. Demandez à l'application de sauvegarder automatiquement votre mot de passe

D. Transférez sans vérifier le montant



4. Pourquoi est-il dangereux d'utiliser le Wi-Fi public pour les transferts numériques de fonds ?

Une seule réponse est correcte !

A. Il est trop lent pour les transactions importantes

B. Il permet des accès non autorisés à vos données sensibles

C. La connexion nécessite un mot de passe

D. Il ne prend pas en charge les paiements en ligne



5. Que faire si vous constatez une anomalie dans l'historique de vos transactions ?

Une seule réponse est correcte !

A. Ignorez-le et attendez qu'il se résolve de lui-même.

B. Supprimez l'application et réinstallez-la.

C. Contactez immédiatement votre banque ou l'assistance de votre app.

D. Essayez d'annuler la transaction vous-même.



6. Laquelle des propositions suivantes est une caractéristique essentielle de l'historique des transactions ?

Une seule réponse est correcte !

A. Envoi d'argent à plusieurs destinataires

B. Affichage des détails tels que la date, le montant et les numéros de référence

C. Dépôt d'espèces sur un compte

D. Ajout de nouveaux moyens de paiement



7. Parmi les éléments suivants, lequel est le signe d'une tentative d'hameçonnage ?

Une seule réponse est correcte !

A. Un e-mail avec un libellé urgent demandant des informations personnelles

B. Un site Web sécurisé avec une icône de cadenas dans la barre d'adresse

C. Une notification de votre application bancaire concernant une transaction récente

D. Un message provenant d'un contact connu sans aucun lien suspect





IMOBILE
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 toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive « Éducation, audiovisuel et culture » (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenus responsables. Numéro de projet : 2023-1-RO01-KA220-ADU-000157797