

Conseils de Sécurité de COPEDU

1. **Protégez les informations de votre compte**

- Ne partagez jamais votre mot de passe, votre code PIN ou votre OTP avec qui que ce soit.
- Utilisez des mots de passe forts (mélange de lettres majuscules, lettres minuscules, chiffres et caractères spéciaux. Ex : Secure@2025).
- Changez régulièrement vos mots de passe.

2. **Méfiez-vous des tentatives d’hameçonnage (phishing)**

- Ne cliquez pas sur des liens suspects dans les e-mails ou messages.
- Vérifiez toujours les e-mails prétendant provenir de la banque.
- Copedu ne vous demandera jamais vos informations de connexion par e-mail ou téléphone.

3. **Sécurisez vos appareils**

- Installez et mettez à jour un logiciel antivirus sur vos appareils.
- Gardez votre système d’exploitation et vos applications bancaires à jour.
- Évitez d’utiliser le Wi-Fi public pour les services bancaires en ligne.

4. **Surveillez vos transactions**

- Vérifiez régulièrement vos relevés bancaires pour détecter toute transaction non autorisée.
- Configurez des alertes SMS ou e-mail pour toutes vos transactions.
- Signalez immédiatement toute activité suspecte.

5. **Méfiez-vous des appels et messages frauduleux**

- Les employés de Copedu ne vous appelleront jamais pour demander des informations sensibles (exemple : mot de passe, code PIN, etc.).
- Vérifiez toute demande inhabituelle en appelant la ligne d’assistance officielle de Copedu : +250 788 319 829.
- Ne répondez pas aux messages de loterie ou de gain prétendant provenir de Copedu.

6. **Protégez les informations de votre carte bancaire**

- Couvrez le clavier lorsque vous entrez votre code PIN aux distributeurs automatiques (ATM).
- Ne notez pas votre code PIN et ne le stockez pas sur votre téléphone.