LES BANQUES AFRICAINES FACE À LA CYBERCRIMINALITÉ : QUELLE GESTION ?



I - Définition de la cybercriminalité



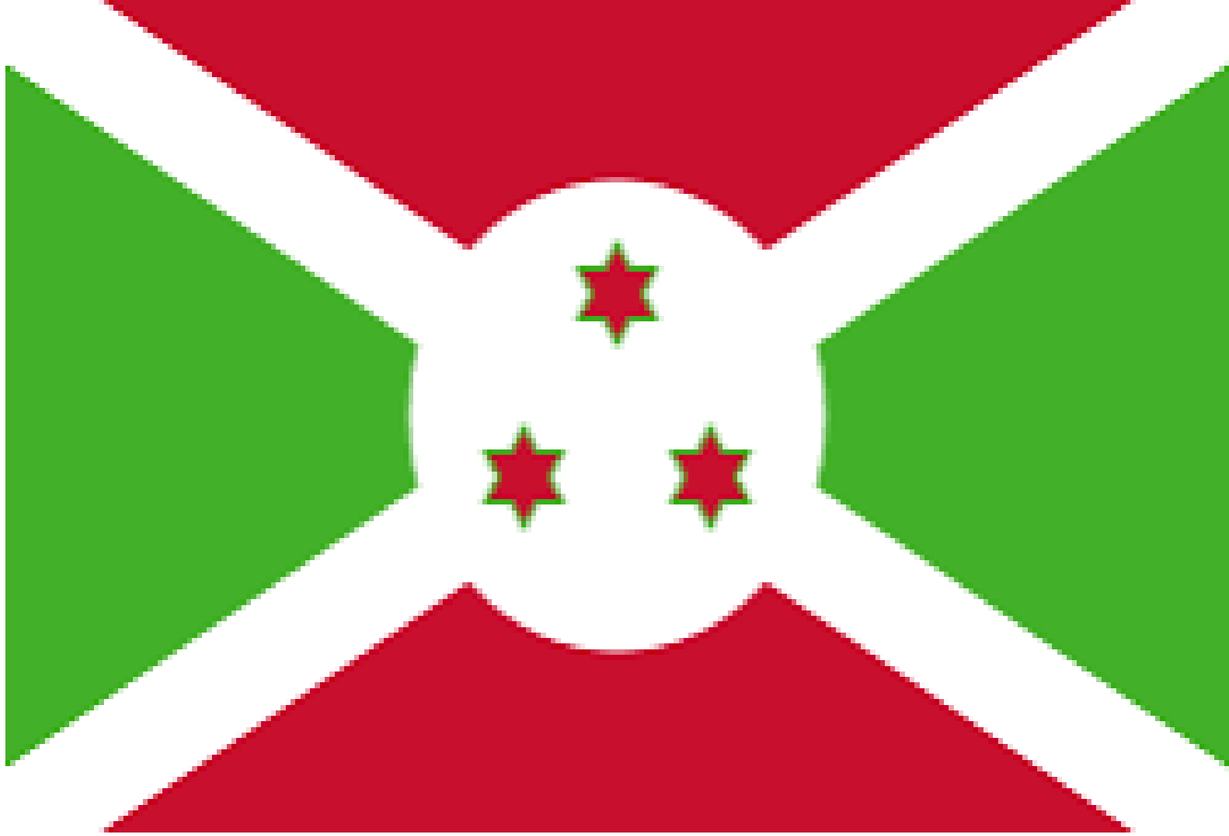
1.1. EN RDC :



La cybercriminalité est l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication... dont la commission est facilitée ou liée à l'utilisation des technologies. (Ordonnance-Loi n° 23/010 du 13 mars 2023 portant Code du Numérique, article 2, alinéa 24)



1.2. AU BURUNDI :



Tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent. (Loi n° 1/10 du 16 mars 2022 portant prévention et répression de la cybercriminalité)



2. Approche du FM

L'Institution aborde la cybercriminalité sous l'angle de la stabilité financière et macroéconomique plutôt que par sa définition juridique. Le FMI traite le risque cybercriminalité comme une menace pouvant utiliser les vulnérabilités de la stabilité financière, à travers les canaux de transmission (*channels of transmission*) :

1

Directement, vol massif de fonds → paralysie d'un système de paiement

2

Indirectement, perte de confiance des déposants → retraits massifs, contagion des parties prenantes interconnectées (banques, systèmes de compensation, marchés), interruption des mécanismes critiques de paiement et de règlement-livraison...



Les modalités de gestion proposées par le Fonds se déclinent autour de :

✓ **1**

établissement d'un cadre légal et réglementaire spécifique pour le risque cybercriminalité.

✓ **2**

développement d'exercices de stress test.

✓ **3**

coordination entre toutes les parties concernées.



3. Approche du Comité de Bâle



Le Comité de Bâle introduit le traitement de ce risque dans le risque opérationnel.

Pour rappel, le risque opérationnel est le risque de pertes résultant de processus, systèmes ou personnes inadéquats ou défaillants, ou d'événements externes (cyber-attaques).

La réponse des banques doit être la cyber-résilience (capacité d'une banque à assurer la continuité de ses services et prestations en cas de dysfonctionnement dû à une attaque malveillante cybercriminelle).

L'exercice de typologies des actes cybercriminels fait ressortir un éventail large d'infractions :

- visant les systèmes informatiques (intrusions, piratage et sabotage des données, dénis de service distribué pour créer des perturbations (DDoS Distributed Denial Of Service, interception de communication)

- visant le contenu (contenus illicites, cyberharcèlement, désinformation)

- à but lucratif / cybercriminalité économique (fraude à la carte bancaire, escroquerie en ligne, rançongiciels ou ransomware, blanchiment via crypto-monnaies)

- la propriété intellectuelle (piratages de logiciels, contrefaçon numérique)

- d'atteintes aux personnes (usurpation d'identité numérique, vols de données personnelles, sextorsion)

- de cybercriminalité étatique (sabotages d'infrastructures critiques comme le système SWIFT)

II - Gestion de la cybercriminalité dans une banque



2.1. Les acteurs promoteurs du cadre réglementaire

Sont le Régulateur (Banque Centrale), le Superviseur (Commission Bancaire ou équivalent - l'Autorité en charge du Marché Financier), l'Agence Nationale en charge de la cybersécurité, la Direction Générale du Trésor.

Ce sont ces acteurs qui élaborent les règles de gestion des risques ‘‘Cyber et Technologies de l'Information et de la Communication TIC dans le secteur Banque-Finance’’

Ces normes sont destinées aux banques, établissements financiers, établissements de microfinance et de monnaie électronique, fintechs, prestataires tiers critiques comme les TIC (cloud, logiciels, data centers).

En Europe, les 5 piliers du règlement sur la résilience opérationnelle numérique du secteur financier – **DORA** (*Digital Operational Resilience Act*), entré en vigueur le 27 décembre 2022 et appliqué depuis le 17 janvier 2025, sont :

✓ Gouvernance et gestion des risques (responsabilités des organes et cartographies des risques cyber).

✓ Respect des délais de notification des incidents majeurs (4h de temps pour la notification initiale, ensuite 72h pour le rapport intermédiaire et 1 mois pour le rapport final).

✓ Réalisation de tests de résilience opérationnelle (Test d'intrusion fondé sur menace réelle - *Threat-Led Penetration Testing-TLPT)*.

✓ Suivi du risque prestataires tiers (tenue obligatoire d'un registre).

✓ Partage d'informations sur les cybermenaces, action volontaire pour favoriser le développement d'une défense sectorielle coordonnée.

Le dispositif a prévu des sanctions fortes :

- 2 % du chiffre d'affaires annuel mondial pour une entité financière.

- 1 % du chiffre d'affaires mondial quotidien moyen pour un prestataire tiers TIC critique désigné.

Dans certaines juridictions, des projets sont en cours pour exiger aux banques :

- Une vraie gouvernance du dispositif de cybersécurité formalisée, ainsi qu'une gestion proactive des risques cyber.

L'Organe de Direction/l’Organe délibérant selon le cas, est le responsable ultime du cadre de gestion, avec les procédures d'identification et d'atténuation de ces risques, de programmation et de réalisation des tests de résilience opérationnelle numérique.

Chaque banque doit mettre en œuvre et documenter l'articulation entre sa stratégie globale et la stratégie de résilience numérique spécifique.

Toutes les politiques et procédures doivent être écrites concernant notamment le chiffrement, les actifs informatiques, les opérations, le contrôle d'accès.

Les modalités de gestion du risque cyber peuvent comporter le réexamen annuel obligatoire du cadre, la description des modifications apportées, les conclusions, l’analyse de la gravité des faiblesses et lacunes trouvées, la présentation des mesures de remédiation, les canevas des rapports et des déclarations requises.

D’autres juridictions ont elles aussi avancé significativement sur ce chantier en mettant à disposition un mécanisme dédié.

Il ressort de la revue que la réponse à la cybercriminalité passe par :

- L'existence d'une fonction cybersécurité.

- La désignation d'un Responsable de la Sécurité du Système d'Information (idéalement nommé par le Directeur), après approbation du Conseil d'Administration, sa mobilité (mutation, révocation) fait également l'objet d’une délibération du Conseil.

…Il peut être rattaché au plan hiérarchique au Directeur Général et fonctionnellement au Conseil. Dans ce schéma, le Responsable en dernier ressort du dispositif de cybersécurité est l'organe délibérant.

- L'élaboration et l'adoption d'une Stratégie et d'une Politique de Sécurité du Système d'Information;

- L'efficacité du dispositif de cybersécurité, la cartographie des risques, l'appétence au risque, la mesure d'identification, d'évaluation des risques et les mesures de remédiation;

- La disponibilité d'un staff dédié et conforme à la taille de la banque, à son exposition et au volume de ses activités;

- L'intégration des scénarii de cybersécurité aux exercices de simulation de crise périodiques.

- La formation et la sensibilisation des parties prenantes sur leurs rôles et responsabilités.

- La révision régulière du programme de cybersécurité.

- La bonne information du Conseil d'Administration sur les événements en lien avec les risques technologiques ainsi que sur l'émergence de nouvelles menaces.

- Le bon entretien des liens de la fonction cybersécurité avec les fonctions ‘‘Gestion des risques’’, ‘‘Conformité’’, ‘‘Audit interne’’ et ‘‘Informatique’’;

- La définition claire, pour les banques, des composantes de la stratégie cyber, sa politique, son programme, son plan de formation et de sensibilisation.

III - Gestion du risque cyber



La gestion du risque cyber est fondée sur :

- Les référentiels figurant au socle documentaire ;
- Les principes majeurs retenus pour garantir la prévention ‘‘des défaillances, obsolescences, erreurs de configuration’’, et autres dysfonctionnements ;
- Le reporting régulier au Conseil d'Administration.

À cet effet, il est entretenu en permanence une veille tirée de différentes sources jugées fiables (Centres d'alerte, abonnements spécifiques, partage d'information entre consœurs...).

l'identification des risques cyber est nécessairement assortie de l'évaluation de leur impact à rythme régulier.

Les mesures portent sur :

- protection contre les cybermenaces ;
- cadre de gestion des actifs informatiques ;
- règles de gestion et de conduite des projets et programmes informatiques ;

- configurations et architectures sécurisées ;

- sécurité des interfaces applicatives programmées ;

Les modalités de gestion des identités et accès, et d'accès distant au système d'information ;

- de conditions claires et précises d'externalisation des prestations de services informatiques essentiels (cloud computing, analyse des contrats, des risques, sous-traitance...).

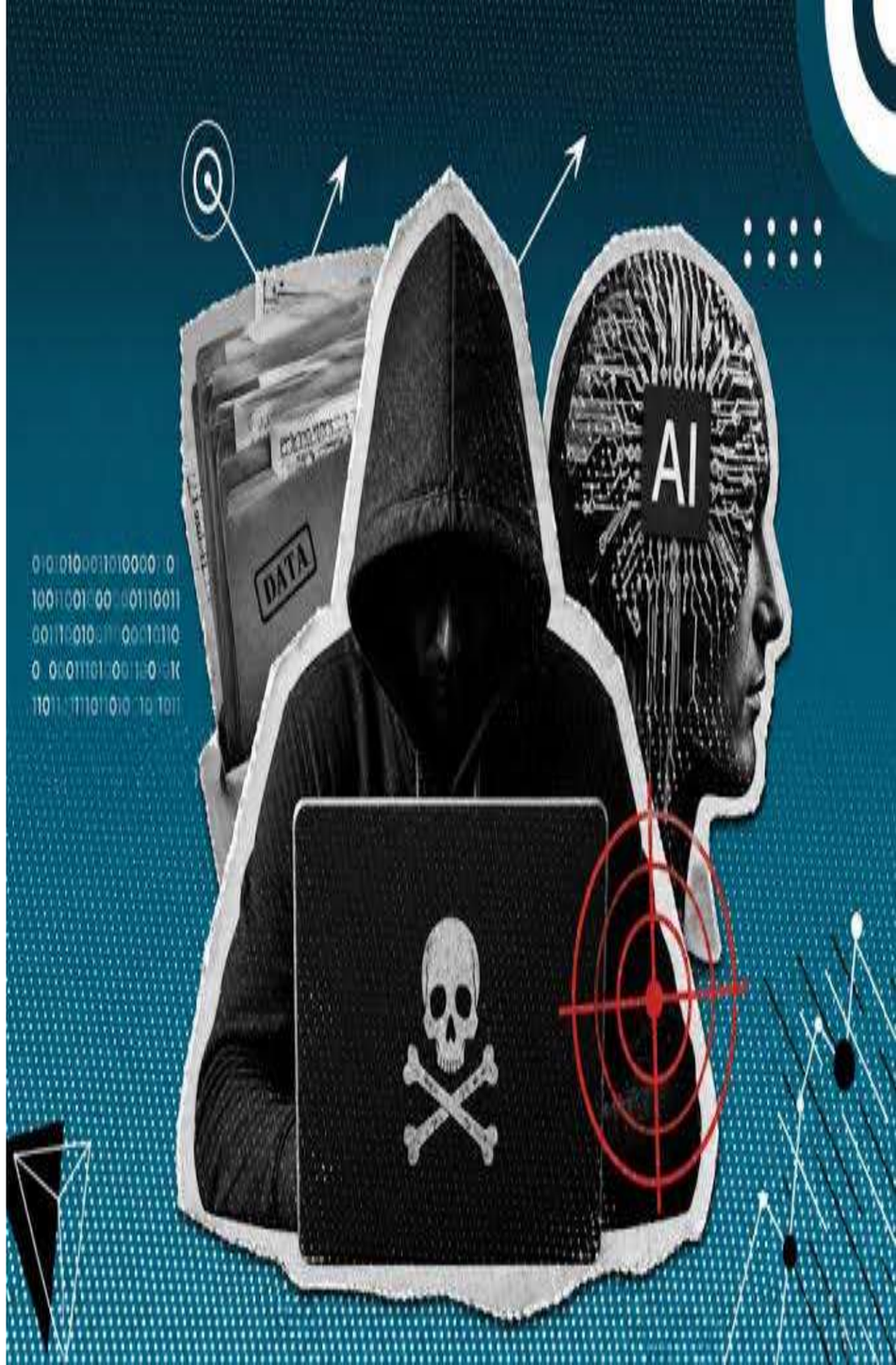
Chaque banque est tenue à la surveillance de ses systèmes, à l'utilisation efficace des alertes et à la détection des incidents de cybersécurité. À cet effet, elle devra développer, louer ou acquérir tous les moyens/outils nécessaires.

Elle doit disposer d'une procédure de traitement des cyber-incidents, qui est la base de sa cyber-résilience.

Elle prévoit le plan de continuité d’activité en cas de cyber-incident et le plan de reprise d’activité, composantes du PCA global.

Dans l'intervalle, la réalisation des tests d'intrusion dans le système d'information doit être codifié et les dispositions y contenues strictement suivies.

IV- Impacts de l'IA sur la croissance de la cybercriminalité et Réponses des banques



1

“En banque, l'IA a changé la guerre. Avant c'était le « brouteur » avec un faux mail.
Maintenant, c'est une usine industrielle.”

2

“L'IA est-elle le catalyseur de la cybercriminalité bancaire ou le bouclier défensif de la banque ?”

Aujourd'hui, par l'IA générative :

- le phishing génératif est quasi parfait (le mail n'est plus bourré de fautes ou d'erreurs sur les noms des gestionnaires);

- le deepfake vocal (l'IA clone la voix des clients ou des supérieurs hiérarchiques);

- les tests massifs sur les codes (plus de 100 mille par l’IA) finissent par avoir raison des combinaisons très sophistiquées;

- le malware généré par l'IA peut étudier les habitudes sur un compte pendant plusieurs mois avant de le vider en un seul jour

- la création de comptes mules avec de fausses pièces d'identité;

- la dépendance aux SMS OTP (One Time Password, mot de passe à usage unique envoyé par SMS) crée des proies faciles pour l’IA;

- la faible maturité (robustesse) du SOC (Security Operations Center) permet à l'IA de déceler très rapidement les points de faiblesse, en raison de la capacité de détection du système, de qualification et de réponse aux incidents de cybersécurité.

Cette situation est due à la couverture insuffisante des actifs numériques, à une automatisation limitée et à des procédures de réponse de niveau inadapté.

Les conséquences sont pour la banque :

- la recrudescence des fraudes ;
- les compromissions multiples de comptes ;
- les attaques rançongiciels ;
- les intrusions.

Aujourd'hui, les banques peuvent aussi utiliser l'IA pour organiser leurs réponses :

- par analyse de comportement, l'IA permet de bloquer instantanément les comptes et les transactions suspectes;

- par la biométrie comportementale (de manière de taper le code et de bouger la souris);

- par la génération des tokens dynamiques (petites unités de texte utilisées pour lire et générer du contenu);

- par l'authentification comme FIDO2 (standard d'authentification qui permet de se connecter à un service sans mot de passe).

Les recommandations fortes sont :

- Mettre en place une architecture à au moins trois (3) niveaux (Prévention - Détection - Réponse)

- Faire les investissements nécessaires en fonction de la taille de la banque et du volume des activités (actifs numériques, effectifs adéquats)

- Structurer une gouvernance efficace;

- Recourir au Scoring IA (pour aligner l'IA sur les besoins stratégiques de la banque, pour s'ajuster aux réalités du terrain, pour avoir une évaluation struturée des données, pour faciliter les prises de décisions grâce à une approche basée sur des critères mesurables);

- Bâtir une culture cyber pour le personnel, les dirigeants, les administrateurs, les prestataires et les autres parties prenantes.

PRODUIT DANGEREUX · LOT 2026

EDITH BROU BLEU

DANGER

Arnaques numériques en Côte d'Ivoire

Nocif pour votre compte. Contient 8 pièges.





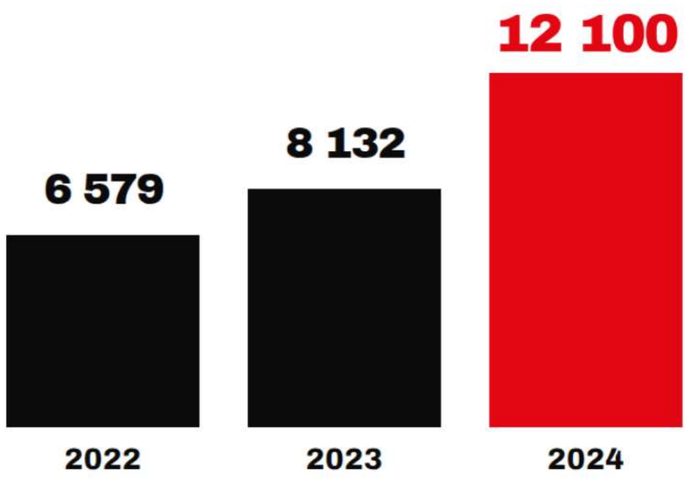
Composition : 60 % promesse, 30 % pression, 10 % faux logo. Tenir hors de portée de vos codes secrets.

225 · 2026 · 08 · CI

Mode d'emploi

Faites défiler pour vous protéger →

LES PLAINTES ONT PRESQUE DOUBLÉ EN DEUX ANS



Plaintes enregistrées par la PLCC

6,9 Md
FCFA de préjudice déclaré en 2024

36 %
des plaintes concernent des femmes

Attention

Ce ne sont que les victimes qui osent porter plainte. La honte fait taire les autres.

Toutes infractions cyber confondues · Source : ANSSI / PLCC, bilan.gouv.ci, juillet 2025

LE FAUX CADEAU

503

plaintes contre un seul réseau · 231 M FCFA volés

MODE D'ACTION

Un SMS annonce un gain de 37 000 FCFA. Le lien ouvre un faux formulaire qui réclame votre numéro et votre code secret. Le compte est vidé.



Antidote

Un vrai cadeau ne demande jamais votre code secret. Ne cliquez pas.

Source : PLCC, via Agence Ivoirienne de Presse

LE FAUX SERVICE CLIENT

10 M

FCFA de préjudice · réseau démantelé à San Pedro, avril 2026

MODE D'ACTION

Vous recevez un code par SMS. Aussitôt, un faux agent appelle : « lisez-moi le code, c'est pour la mise à jour ». Ce code lui ouvre votre compte.



Antidote

Raccrochez. Rappelez vous-même le numéro officiel (Wave : 1315).

Sources : Police / BRI de San Pedro via AIP, avril 2026 · Wave Côte d'Ivoire

LA PUCE VOLÉE

5,1 M

FCFA volés à une commerçante · septembre 2026

MODE D'ACTION

L'escroc repère votre numéro, par exemple pendant un live TikTok. Avec de faux papiers et un complice en agence, il obtient une nouvelle puce à votre nom.



Antidote

Ligne coupée sans raison ? Appelez votre opérateur tout de suite, depuis un autre téléphone.

Source : PLCC, via AIP et Yessouan, 18 septembre 2026

LE PROCHE PIRATÉ

1 205

comptes e-mail ou Facebook piratés signalés en 2024

MODE D'ACTION

Le message vient du vrai compte d'un proche : une urgence, un transfert « juste pour aujourd'hui ». Le compte a été piraté. C'est l'escroc qui écrit.



Antidote

Appelez la personne sur un numéro déjà connu. Jamais dans la même conversation.

Source : bilan PLCC 2024, via KOACI, mai 2025

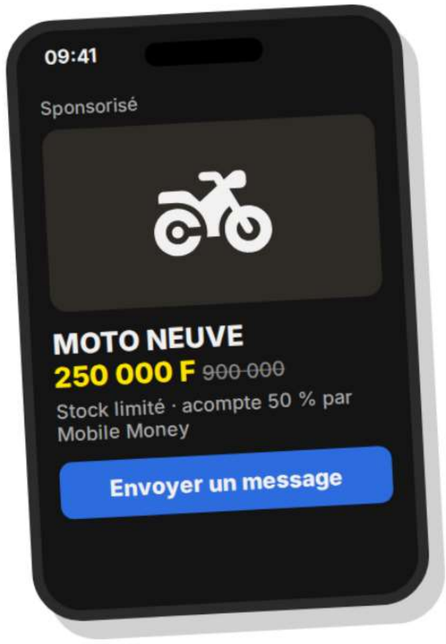
LA FAUSSE BONNE AFFAIRE

222

plaintes contre un seul réseau de fausses ventes de motos

MODE D'ACTION

Moto à prix cassé, chambre d'hôtel : l'annonce paraît sérieuse. Vous versez un acompte, le vendeur disparaît. En août 2026, un escroc copiait les pages de vrais hôtels.



Antidote

Pas d'acompte avant d'avoir vu le bien. Réservez par le site ou le numéro officiel.

Sources : PLCC (page officielle) · KOACI, faux hôtels, 21 août 2026

LE PLACEMENT MIRACLE

0

plateforme crypto agréée en Côte d'Ivoire à ce jour (État, août 2026)

MODE D'ACTION

Gains « garantis », premiers retraits payés pour gagner votre confiance, puis le site ferme. Sunpower a piégé plus de 1 000 personnes. Le scénario revient avec la crypto.



Antidote

Gain rapide et garanti = arnaque. Signalez au 8000 10 10 (numéro vert).

Sources : Comité de veille sur les placements financiers illicites, 17 août 2026 · PLCC via AIP

LA VIDÉO TRUQUÉE

200 000 F

« par jour » : la promesse d'une vidéo truquée d'un grand banquier ivoirien

MODE D'ACTION

L'IA fait parler des personnalités : patron de banque, présentateur télé, et même le chef de l'État en mars 2026. La vidéo mène à un faux site d'investissement.



Antidote

Une célébrité vous promet de l'argent en vidéo ? Arnaque. Vérifiez sur ses comptes officiels.

Sources : Fraternité Matin, 13 mars 2026 · Digital Business Africa, 4 mars 2026

L'AMOUR À DISTANCE

144 M

FCFA extorqués dans un seul dossier démantelé (décembre 2025)

MODE D'ACTION

Un profil séduisant, des mois de messages tendres. Puis l'urgence : héritage bloqué, frais de douane, billet d'avion. Les photos intimes servent ensuite au chantage.



Antidote

On ne paie jamais pour être aimé. Gardez les preuves, cessez de payer, parlez-en.

Source : KOACI, 20 décembre 2025

4 VARIANTES À RECONNAÎTRE



Le faux concours

« Admission garantie » à un concours contre de l'argent. 120 victimes, 74 M FCFA (mai 2026).



La fausse autorité

Logo d'une banque, d'un ministère ou de la PLCC pour réclamer des frais ou vos codes.



Le faux remboursement

« Je me suis trompé de numéro, renvoyez l'argent. » Vérifiez d'abord votre solde dans l'appli.



Le chantage aux images

Menace de publier des photos intimes. Payer n'arrête rien : gardez les preuves, portez plainte.

Sources : PLCC via Afrique sur 7 (mai 2026) · Orange CI « Stop arnaques »

8 ARNAQUES, UNE SEULE FORMULE

1 L'APPÂT

un cadeau, un prix cassé, un gain, de l'amour, une urgence

+ LA FAUSSE CONFIANCE

un logo, un « agent », le compte d'un proche, une célébrité

+ LA PRESSION

« tout de suite », « ne dites rien », « dernière chance »

= LE VOL

votre code, votre mot de passe, un transfert Mobile Money

Règle d'or

On vous presse de payer pour « débloquer » un paiement ? Stop.

5 RÉFLEXES CONTRE LES 8 PIÈGES

P01 Je ne donne jamais mon code secret, mon code SMS ou mon mot de passe.

P02 Je ne clique pas sur un lien reçu pour un cadeau, un gain ou une mise à jour.

P03 Je rappelle moi-même : le proche sur son numéro connu, le service sur le numéro officiel.

P04 Je ne verse pas d'acompte pour un bien que je n'ai pas vu.

P05 Je refuse tout gain rapide et garanti, même promis par une célébrité.

À garder

Enregistrez ce post et envoyez-le à vos parents.

VICTIME ? AGISSEZ DANS L'HEURE

1 BLOQUEZ

Appelez le service client officiel de votre opérateur ou banque. Changez vos codes dans l'appli officielle.

2 GARDEZ TOUT

Captures, numéros, liens, reçus, références de transaction, date et heure.

3 PORTEZ PLAINTE

À la PLCC, à la police ou à la gendarmerie, avec vos preuves.

NUMÉROS UTILES

1315
service client Wave

8000 10 10
placements illicites · gratuit

Deuxième arnaque

On vous promet de « récupérer » votre argent contre des frais ? C'est encore une arnaque.

ARNAQUER EST UN DÉLIT

ESCROQUERIE

1 à 5 ans

de prison

jusqu'à 3 M FCFA d'amende

Code pénal, art. 471

CHANTAGE

1 à 5 ans

de prison

jusqu'à 3 M FCFA d'amende

Code pénal, art. 475

USURPATION D'IDENTITÉ

2 à 5 ans

de prison

5 à 10 M FCFA d'amende

Loi n° 2013-451, art. 19

HAMEÇONNAGE

1 à 5 ans

de prison

jusqu'à 100 M FCFA ; 5 ans minimum si des fonds sont détournés

Loi n° 2013-451, art. 25

Peines prévues par les textes ; le tribunal décide au cas par cas.

UNE ARNAQUE PARTAGÉE EST UNE ARNAQUE QUI ÉCHOUE

Partagez ce guide

à quelqu'un qui utilise le Mobile Money. Donc à tout le monde.

Racontez en commentaire

quelle arnaque vous avez reçue cette semaine.

Sources et crédits

Faits vérifiés au 28 septembre 2026 : ANSSI / PLCC (bilan 2024), Agence Ivoirienne de Presse, KOACI, Fraternité Matin, Comité de veille sur les placements financiers illicites, Wave et Orange Côte d'Ivoire, Code pénal et loi n° 2013-451. Liens complets dans les notes et en commentaire. Bilans annuels et affaires individuelles ne s'additionnent pas ; ordre des pièges éditorial.

Illustrations : créations originales · Icônes Font Awesome (CC BY 4.0) · Polices Archivo, Inter, IBM Plex Mono (licence OFL) · Aucune photo tierce.

JE VOUS REMERCIE POUR VOTRE ATTENTION ET VOTRE INDULGENCE

