GSS

GLOBAL SYNERGIES SOLUTIONS

ÉDITION 2026–2027



SENTINELLE™

Le guide de la confiance numérique

Protéger son argent, ses données et ses institutions face aux arnaques et aux cyberattaques.

دليل الثقة الرقمية

Citoyens | Entreprises | Banques | Administrations | ONG

Une publication de Global Synergies Solutions SAS
Le choix intelligent pour votre transformation

gssynergies.com

ÉDITORIAL

La confiance numérique, ça s'apprend.

Mobile money, banque en ligne, messageries, services publics numériques : notre quotidien passe désormais par un écran. Les escrocs l'ont compris. Ils ne « piratent » presque jamais : **ils trompent**. SENTINELLE™ réunit les pièges les plus courants et les réflexes simples qui permettent de les déjouer, pour chacun de nous et pour nos organisations.

SOMMAIRE

01 Les 5 pièges les plus fréquents — Reconnaître les arnaques — p. 3

02 Les 12 réflexes SENTINELLE™ — Pour tous, au quotidien — p. 6

03 Entreprises — Le tableau de bord du dirigeant — p. 8

04 Banques et établissements financiers — Un environnement sécurisé — p. 9

05 Administrations et ONG — Deux missions, mêmes exigences — p. 10

06 Fiche d'urgence — Les 5 gestes de la première heure — p. 11

07 Aller plus loin avec GSS et CyberScore 360° — Évaluer, former, protéger — p. 12

COMMENT LIRE CE GUIDE

ROUGE · DANGER — La technique utilisée par l'escroc.

ORANGE · ALERTE — Le signal qui doit vous faire douter.

VERT · BON RÉFLEXE — Ce qu'il faut faire pour se protéger.

BLEU · REPÈRE — Les informations et les définitions.

Citoyens p. 3 à 7 et 11

Entreprises p. 8 et 11

Banques p. 9 et 11

Administrations p. 10 et 11

ONG p. 10 et 11

1. Reconnaître — Identifier les scénarios d'arnaque avant qu'ils ne fonctionnent.

2. Prévenir — Adopter des réflexes simples, chez soi comme au travail.

3. Réagir — Savoir quoi faire, et vite, quand l'incident survient.

PARTIE 01

Les 5 pièges les plus fréquents

Chaque arnaque suit le même scénario : une situation banale, une manipulation, un signal d'alerte, et un réflexe qui l'aurait déjouée.





PIÈGE 01

Le faux transfert mobile money

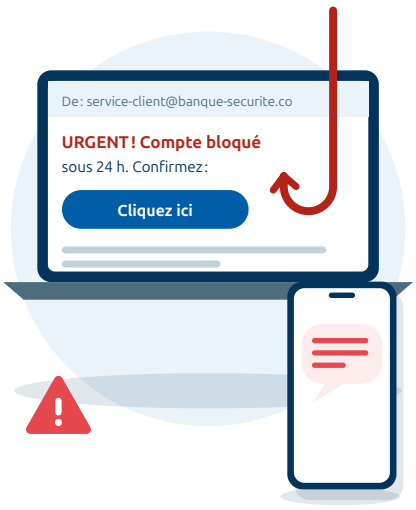
SITUATION →
Vous recevez un SMS annonçant un dépôt sur votre compte mobile money.

LA FRAUDE →
Le SMS est faux. Un appel insistant vous demande ensuite de « rembourser » l'argent envoyé « par erreur ».

SIGNAL D'ALERTE →
Le message vient d'un numéro ordinaire, pas de l'expéditeur officiel de l'opérateur. On vous presse.

BON RÉFLEXE
Vérifiez votre solde dans l'application ou le menu officiel. Ne renvoyez rien : une vraie erreur se règle avec l'opérateur.

Un SMS ne prouve rien. Seul votre solde officiel fait foi.



PIÈGE 02

L'hameçonnage (phishing)

SITUATION →
Un e-mail, un SMS ou un message semble venir de votre banque, de votre opérateur ou d'une administration.

LA FRAUDE →
Un lien mène vers un faux site, copie du vrai, qui vole vos identifiants ou les données de votre carte.

SIGNAL D'ALERTE →
Menace ou urgence, expéditeur étrange, fautes, lien raccourci ou adresse qui imite la vraie.

BON RÉFLEXE
Ne cliquez pas. Ouvrez vous-même l'application officielle ou tapez l'adresse du site que vous connaissez.

Le bon lien, c'est celui que vous tapez vous-même.



PIÈGE 03

Le vol de compte WhatsApp

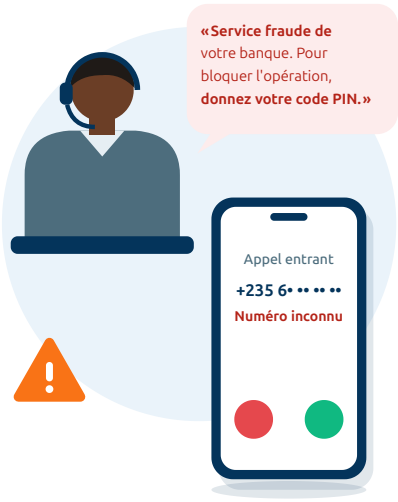
SITUATION →
Un contact vous écrit: il vous aurait envoyé un code «par erreur» et vous demande de le lui transférer.

LA FRAUDE →
Ce code active votre compte sur son téléphone. L'escroc écrit ensuite à vos proches en votre nom.

SIGNAL D'ALERTE →
On vous réclame un code reçu par SMS, même un «ami»: son compte a peut-être déjà été volé.

BON RÉFLEXE
Ne transmettez jamais ce code. Activez la validation en deux étapes: Paramètres › Compte.

Un code reçu par SMS ne se partage jamais. Avec personne.



PIÈGE 04

Le faux conseiller bancaire

SITUATION →
Un «conseiller» ou un «service fraude» vous appelle au sujet d'une opération suspecte.

LA FRAUDE →
Il connaît parfois votre nom ou votre agence, puis réclame votre code PIN, un code SMS ou une «validation d'annulation».

SIGNAL D'ALERTE →
Demande de code confidentiel, pression, interdiction de raccrocher ou de contacter votre agence.

BON RÉFLEXE
Raccrochez. Rappelez votre banque au numéro inscrit au dos de votre carte ou rendez-vous en agence.

Votre banque ne vous demandera jamais votre code PIN.



PIÈGE 05

Le rançongiciel

SITUATION →
Une pièce jointe, une clé USB ou un logiciel piraté est ouvert sur un poste de l'organisation.

LA FRAUDE →
Un programme malveillant chiffre les fichiers, souvent jusqu'aux serveurs partagés, puis une rançon est exigée.

SIGNAL D'ALERTE →
Fichiers illisibles ou renommés, extensions inconnues, message de rançon, ordinateur anormalement lent.

BON RÉFLEXE
Isolez le poste du réseau, alertez l'informatique, ne payez pas. Des sauvegardes hors ligne permettent de repartir.

Sans sauvegarde hors ligne, pas de plan B.

LE TEST SENTINELLE™ · 10 SECONDES

Avant de répondre, de cliquer ou de payer, posez-vous 3 questions.

1
On me presse ?
« Vite », « aujourd'hui », « sinon votre compte sera bloqué ».

2
On me demande un code ou de l'argent ?
PIN, code SMS, transfert, frais « de déblocage ».

3
On me demande le secret ?
« N'en parlez pas », « ne raccrochez pas ».

Un seul « oui » suffit : j'arrête tout et je vérifie auprès d'une source officielle.

AVANT / APRÈS · LE RÉFLEXE QUI CHANGE TOUT

✕ Je renvoie l'argent « reçu par erreur ».	→	**Je consulte mon solde dans l'application officielle.**
✕ Je clique sur le lien du message.	→	**J'ouvre moi-même le site ou l'application.**
✕ Je donne le code demandé par téléphone.	→	**Je raccroche et je rappelle le numéro officiel.**

PARTIE 02 · POUR TOUS

Les 12 réflexes SENTINELLE™

Douze gestes simples, valables sur téléphone comme sur ordinateur, à la maison comme au bureau. À retenir, à afficher, à transmettre.



01 Mes codes restent secrets

PIN, mots de passe, codes reçus par SMS : aucun organisme sérieux ne vous les demandera.

✓ **Je ne les dis, ne les écris et ne les transfère à personne.**

02 Je vérifie à la source

Un appel ou un message inattendu peut être faux, même s'il affiche un nom connu.

✓ **Je rappelle l'organisme au numéro officiel que je connais.**

03 L'urgence est une alarme

« Dernier délai », « compte bloqué » : la pression sert à vous empêcher de réfléchir.

✓ **Je prends cinq minutes et j'en parle à un proche.**

04 Des mots de passe longs et uniques

Un mot de passe réutilisé ouvre tous vos comptes s'il fuit une seule fois.

✓ **Une phrase de passe de 12 caractères ou plus, différente par compte.**

05 La double vérification partout

Même avec votre mot de passe, l'intrus reste bloqué sans votre téléphone.

✓ **Je l'active sur ma messagerie, mes réseaux sociaux et ma banque.**

06 Les mises à jour sans attendre

Elles corrigent des failles que les attaquants exploitent déjà.

✓ **J'active les mises à jour automatiques.**

07 Applications officielles uniquement

Une application reçue par lien ou par message peut espionner votre téléphone.

✓ **J'installe seulement depuis Google Play ou l'App Store.**

08 Mon téléphone est verrouillé

Ouvert et perdu, il donne accès à votre argent et à vos messages.

✓ **Code + empreinte, localisation et effacement à distance activés.**

09 Je sauvegarde régulièrement

Panne, vol ou rançongiciel : une copie récente vous sauve.

✓ **Une copie de mes données importantes hors de l'appareil.**

10 Prudence sur les Wi-Fi publics

Un réseau ouvert peut être espionné ou imité.

✓ **Pour la banque et le mobile money, j'utilise mes données mobiles.**

11 Je partage moins en ligne

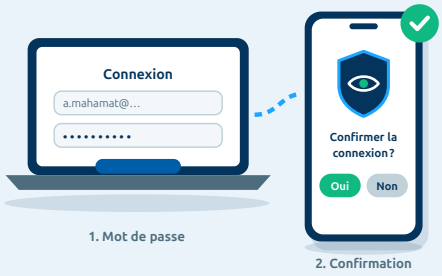
Pièce d'identité, absences, carte bancaire : tout peut nourrir une arnaque.

✓ **Profils en privé ; je réfléchis avant de publier.**

12 Je signale sans honte

Tout le monde peut être piégé. Plus on agit tôt, plus on limite les dégâts.

✓ **J'alerte ma banque ou mon opérateur, puis les autorités.**



ZOOM · RÉFLEXE 05

La double vérification, comment ça marche ?

Pour entrer dans votre compte, il faut **quelque chose que vous savez** (le mot de passe) **et quelque chose que vous avez** (votre téléphone). Un escroc qui vole le mot de passe reste bloqué à la porte.

Ces 12 réflexes existent aussi en affiche autonome (format A3), à imprimer pour les bureaux, agences, écoles et lieux d'accueil.

PARTIE 03 · DIRIGEANTS ET RESPONSABLES

Le tableau de bord du dirigeant

La cybersécurité est une décision de direction, pas seulement un sujet technique. Six questions à poser chaque trimestre à vos équipes.



Cybersécurité · Revue de direction

À compléter chaque trimestre

Sauvegardes

Nos données critiques sont-elles sauvegardées hors ligne, et la restauration est-elle testée ?

Bonne pratique : Règle 3-2-1 : 3 copies, 2 supports, 1 hors ligne. Test de restauration chaque trimestre.

☐ Oui ☐ En cours ☐ Non

Authentification

La double vérification protège-t-elle la messagerie, les accès à distance et les comptes administrateurs ?

Bonne pratique : Double vérification obligatoire pour tous les accès sensibles.

☐ Oui ☐ En cours ☐ Non

Sécurité du réseau

Notre réseau est-il cloisonné et filtré, et le Wi-Fi invités séparé ?

Bonne pratique : Pare-feu à jour, segmentation des zones, accès distants chiffrés.

☐ Oui ☐ En cours ☐ Non

Sensibilisation

Nos collaborateurs savent-ils reconnaître un e-mail ou un appel piégé ?

Bonne pratique : Formation à l'arrivée, rappel annuel et exercices d'hameçonnage simulé.

☐ Oui ☐ En cours ☐ Non

Protection des paiements

Un virement peut-il partir sur la seule base d'un e-mail ?

Bonne pratique : Double validation et rappel téléphonique pour tout changement de coordonnées bancaires.

☐ Oui ☐ En cours ☐ Non

Gestion des incidents

Savons-nous qui appeler, qui décide et quoi faire dans la première heure ?

Bonne pratique : Plan de réponse écrit, contacts à jour, exercice de crise une fois par an.

☐ Oui ☐ En cours ☐ Non

Mesurer avant d'agir. CyberScore 360° vous donne gratuitement une première photographie de votre maturité en cybersécurité. Voir page 12



PARTIE 04 · SECTEUR FINANCIER

La banque sécurisée, en 7 points

Dans la finance, la confiance est l'actif le plus précieux. Elle se protège à chaque maillon de la chaîne.



1 Automates bancaires (GAB)

Dispositifs anti-copie de carte, mises à jour, supervision à distance et contrôle physique régulier.

2 Transactions et paiements

Flux chiffrés, terminaux sécurisés, conformité PCI DSS pour toute donnée de carte.

3 Protection des données

Chiffrement, sauvegardes isolées, accès limité au strict nécessaire.

4 Supervision des systèmes

Centre de supervision (SOC), corrélation des journaux (SIEM), veille 24 h/24.

5 Détection des fraudes

Analyse des opérations carte et mobile money en temps réel, alertes aux clients.

6 Sécurisation des accès

Double vérification, comptes à privilèges contrôlés, revue périodique des droits.

7 Protection contre l'usurpation de marque

Veille sur les faux sites, fausses pages et faux numéros au nom de la banque, avec une procédure de retrait rapide.

CADRE DE RÉFÉRENCE

PCI DSS: norme internationale de sécurité des données de cartes de paiement.
COBAC et BEAC: exigences de la Commission bancaire et de la Banque centrale de la CEMAC applicables aux systèmes d'information et aux moyens de paiement.

MESSAGE À RÉPÉTER À VOS CLIENTS

«Nous ne vous demanderons jamais votre code PIN, ni par téléphone, ni par SMS, ni par e-mail.»

PARTIE 05 · SECTEUR PUBLIC ET HUMANITAIRE

Deux missions, mêmes exigences

Servir les citoyens ou protéger des populations vulnérables : dans les deux cas, une fuite de données peut mettre des personnes en danger.



Administrations

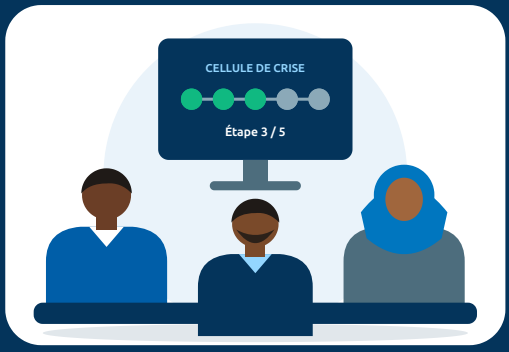


ONG

Administrations		ONG
Souveraineté numérique Données publiques hébergées sous contrôle national ; messagerie officielle souveraine plutôt que messageries grand public.	DONNÉES	**Protection des bénéficiaires** Ne collecter que le nécessaire, avec consentement ; chiffrer les listes et les dossiers.
Classification des informations Public, interne, confidentiel, secret : chaque document a son niveau et ses règles.	CONFIDENTIALITÉ	**Données sensibles** Pas de fichiers de bénéficiaires sur des messageries personnelles ; partage contrôlé et tracé.
Gestion des accès Comptes nominatifs ; un agent qui part, ce sont des accès fermés le jour même.	ACCÈS	**Équipes sur le terrain** Téléphones et tablettes chiffrés, verrouillés et effaçables à distance en cas de perte.
Continuité du service public Plan de continuité, sauvegardes testées, sites officiels protégés contre le défacement.	CONTINUITÉ ET FRAUDE	**Prévention des fraudes** Tout changement de coordonnées bancaires d'un fournisseur se vérifie par téléphone ; double signature.
Coordination en cas d'incident Cellule de crise désignée ; signalement à l'ANSICE, l'agence nationale de cybersécurité.	INCIDENT	**Réponse organisée** Un point focal sécurité, une procédure partagée avec le siège et les partenaires.

URGENCE · À GARDER À PORTÉE DE MAIN

Victime ? Les 5 gestes de la première heure



1. **Coupez le contact**
   Ne répondez plus, ne cliquez plus, ne payez rien.
2. **Bloquez**
   Carte, compte, mobile money ou carte SIM : appelez sans attendre votre banque ou votre opérateur.
3. **Isolez l'appareil**
   Déconnectez-le d'Internet et du réseau (Wi-Fi, câble). Ne l'effacez pas.
4. **Changez vos mots de passe**
   Depuis un autre appareil sain, en commençant par votre messagerie.
5. **Gardez les preuves et signalez**
   Captures d'écran, numéros, références d'opération. Banque, opérateur, police et ANSICE.

ADAPTEZ SELON LA SITUATION

ARGENT

Fraude financière

- Appelez immédiatement l'opérateur ou la banque : blocage et demande d'annulation.
- Notez l'heure, le montant et le numéro du bénéficiaire.
- Déposez plainte au commissariat.

COMPTE

Compte piraté

- Récupérez le compte par la procédure officielle du service.
- Prévenez vos contacts : de faux messages peuvent circuler en votre nom.
- Activez ensuite la double vérification.

ORGANISATION

Attaque informatique

- Isolez les postes touchés du réseau, mais ne les éteignez pas sans avis d'un spécialiste : des preuves sont en mémoire.
- Activez la cellule de crise ; signalez à l'ANSICE.
- Restaurez à partir de sauvegardes saines.

⊘ **À ne pas faire :** payer une rançon, supprimer les messages de l'escroc, réinstaller l'appareil avant analyse, garder le silence par gêne.

PARTIE 07 · ACCOMPAGNEMENT

Aller plus loin avec GSS

Global Synergies Solutions accompagne entreprises, banques, institutions publiques et ONG dans la sécurisation et la transformation de leurs systèmes d'information, au Tchad et au-delà.

SENTINELLE™

Programme de sensibilisation : ateliers, campagnes internes, supports à vos couleurs.

CyberScore 360°

Diagnostic gratuit en ligne de votre maturité en cybersécurité.

Audit 360° du SI

Évaluation de l'infrastructure, des accès, des sauvegardes et de l'exposition.

Formation

Montée en compétences des équipes et exercices de simulation d'attaques.

Conformité

Accompagnement vers les référentiels exigés, dont PCI DSS pour le secteur financier.

Protection et incidents

Solutions de sécurité réseau, veille des menaces et appui en cas d'incident.

GRATUIT · EN LIGNE

Évaluez votre maturité en cybersécurité avec CyberScore 360°.

Scannez le code ou rendez-vous sur le site pour obtenir une première évaluation de votre organisation. Ce diagnostic oriente vos priorités ; il ne remplace pas un audit technique.

gssynergies.com/diagnostic

GSS
GLOBAL SYNERGIES SOLUTIONS

Tél. : (+235) 87 55 55 29 / 30 55 55 29
WhatsApp : (+235) 30 55 55 29
contact@gssynergies.com

www.gssynergies.com
Rue de 40 m, N'Djamena, Tchad
Cybersécurité · IT · Conseil · Énergie

SENTINELLE™ est une marque de Global Synergies Solutions SAS. Reproduction autorisée à des fins de sensibilisation non commerciale, avec mention de la source. Les noms, numéros, montants et adresses figurant dans les illustrations sont fictifs ; les photographies d'illustration ont été générées par intelligence artificielle. Ce guide présente des bonnes pratiques générales et ne remplace pas un conseil adapté à votre situation.