CERT.tg

**RÉPUBLIQUE TOGOLAISE**
**Travail - Liberté - Patrie**

# ALERTE CYBERSECURITE

*ID :* ***202608/AP/13***

**Alerte –** Compromission de comptes **WhatsApp, Facebook (Meta) et autre compte en ligne**
**Date de publication :** 10 Août 2026
**Niveau de Sévérité : Elevé**
**Type de menace :** Compromission de compte / Usurpation d'identité / fraude

CERT.tg a observé une recrudescence des incidents de compromission affectant des comptes utilisateurs de **WhatsApp (standard et Business), Facebook (Meta) et d'autres plateformes en ligne**.
Une précédente alerte envoyée en date du 07/04/2026 signalait déjà cette nouvelle vague d'attaques.

Ces incidents se manifestent notamment par des **déconnexions inhabituelles des utilisateurs de leurs comptes, sans aucune action de leur part**, suivies de tentatives de reconnexion infructueuses. Dans plusieurs cas recensés, les victimes **n'avaient pas activé la vérification en deux étapes (2FA)**, facilitant ainsi la prise de contrôle de leurs comptes par des acteurs malveillants.

Après avoir compromis le compte, les acteurs l'utilisent pour mener des activités malveillantes et parfois changent le numéro, l'adresse mail associée et activent la vérification en deux étapes, empêchant ainsi la victime de reprendre le contrôle de son compte.

Lorsque l'utilisateur victime tente de se reconnecter ou de récupérer son compte, un message peut souvent s'afficher indiquant que **son numéro de téléphone est déjà utilisé, compromis ou banni à la suite d'activités malveillantes**, alors qu'aucune migration ni action de cette nature n'a été effectuée par l'utilisateur.

Ces incidents sont révélateurs d'une **campagne active de tentative de prise de contrôle de comptes**. Les compromissions observées résultent souvent de **campagnes d'ingénierie sociale et de phishing préalables**, visant à obtenir frauduleusement les informations privés ou d'authentification des victimes.

## ➢ Impacts recensés

**Ces incidents entrainent des conséquences suivantes :**

- Prise de contrôle du compte WhatsApp, Facebook (Meta) et autre compte en ligne ;
- Usurpation d'identité de l'entreprise ou du propriétaire du compte ;
- Envoi de messages frauduleux aux contacts ou clients ;
- Propagation de campagnes de phishing ou d'escroquerie ;
- Atteinte à la réputation de l'organisation.

## ➢ Mesures et recommandations

Le CERT recommande aux utilisateurs et aux organisations utilisant WhatsApp, Facebook (Meta) et autre compte en ligne de :

1. Activer la vérification en deux étapes (2FA) dans les paramètres de l'application : ***Réglages > Compte > Vérification en deux étapes, et créer un code PIN personnel ;***
2. Signaler immédiatement tout accès suspect au support officiel de Meta via l'assistance de WhatsApp ;
3. Vérifier les appareils connectés et les sessions actives ;
4. Ajouter une adresse email de récupération à vos comptes;
5. Si votre adresse mail est déjà joint à votre compte WhatsApp, il est recommandé d'activer la double authentification sur cette adresse via les applications « **Google Authenticator ou Microsoft Authentificator** » ;
6. Si vous recevez **des codes de vérifications inattendues ou non-initiés de votre part** veuillez immédiatement signaler puis bloquer le numéro ou l'adresse mail associé ;
7. Ne jamais communiquer ou divulguer vos codes secrets ou informations personnelles aux tierces par appel, sms ou par tout autre moyen, quelle que soit la personne qui le demande ;

**Message de CERT.tg**

1. Les organisations utilisant les plateformes concernées pour leurs communications clients sont invitées à suivre les recommandations formulées tout en sensibilisant leurs équipes sur les vecteurs fréquents de compromission de comptes.
2. En cas d'activité suspecte ou incident cyber, contactez le CERT.tg, 24h/24 7j/7:
    - Tél: +228 70 54 93 25
    - Site officiel : https://cert.tg/ | Mail : incidents@cert.tg

CERT.tg rappelle que la vigilance de chacun contribue à la cybersécurité de tous.

---

**À propos de CERT.tg**

Le **CERT.tg** est le **Centre National de Réponse aux Incidents de Cybersécurité au Togo**. Notre mission est de protéger les citoyens, les organisations et les institutions togolaises contre les menaces cybernétiques en assurant la détection, la prévention et la réponse aux incidents de cybersécurité. Ensemble, faisons du Togo un espace numérique sûr et sécurisé.