

ALERTE CYBERSECURITE

ID : 202601/AP/01

Alerte - Page de phishing

Date de publication : 23/01/ 2026

Niveau de Sévérité : N/A

Type de menace : Phishing / usurpation d'identité/Ingénierie sociale

Le CERT.tg alerte sur une campagne de phishing en cours qui circule via des messages électroniques et/ou réseaux sociaux, prétendant annoncer un recrutement au sein de l'Institut National de la Statistique et des Études Économiques et Démographiques (INSEED).

Le message redirige les cibles vers un site frauduleux accessible via ce lien :

hxxps://tinyurl[.]com/lnseed-Recrutement-2026

Le lien redirige vers un site qui se présente comme un portail de recrutement de l'INSEED, mais qui :

- N'est pas officiel et n'a aucune relation avec l'INSEED du Togo, ni à aucun autre institut national de statistique dans d'autres pays.
- Incite les visiteurs à partager le lien vers leurs contacts pour avancer dans le processus.

En outre, Les éléments analysés confirment que cette campagne ne provient pas de l'INSEED du Togo et ne présente aucun lien officiel ou partenarial avec des institutions statistiques nationales, régionales ou internationales.

[Attention, ne pas cliquez sur le lien, ni fournir d'informations demandées sur cette page]

Risques identifiés :

1. Collecter des informations personnelles ou sensibles des utilisateurs.
2. Éventuellement infecter les terminaux avec des contenus malveillants.
3. Propager le lien malveillant via des contacts ou réseaux sociaux.
4. Exfiltration potentielle de données sensibles et fraudes associées

Actions recommandées :

1. Pour les utilisateurs :

- Ne cliquez jamais sur le lien suspect ou sur toute redirection provenant de ce message.
- Ne fournissez aucune information personnelle (identité, contacts, documents, etc.).
- Ne transférez pas ce message à vos contacts.
- Vérifiez toujours les offres de recrutement uniquement via les sites et communications officiels de l'INSEED :
 - ❖ Site officiel : <https://inseed.tg>
- Signaler tout lien ou page suspect au CERT Togo.

2. Pour toute organisation / entreprise :

- **Isoler et bloquer les URL** malveillantes sur les solutions de sécurité (*proxy, filtrage web*).
- Toujours activer et configurer le *SPF / DKIM / DMARC* sur les domaines pour réduire l'usurpation d'identité email.
- **Sensibiliser** les utilisateurs au phishing et aux faux sites.

Message du CERT.tg aux entités togolaises

En cas de doute, contactez le CERT.tg :

- Ligne directe : +228 70 54 93 25
- Site officiel : <https://cert.tg/> | Mail : incidents@cert.tg

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

À propos du 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.

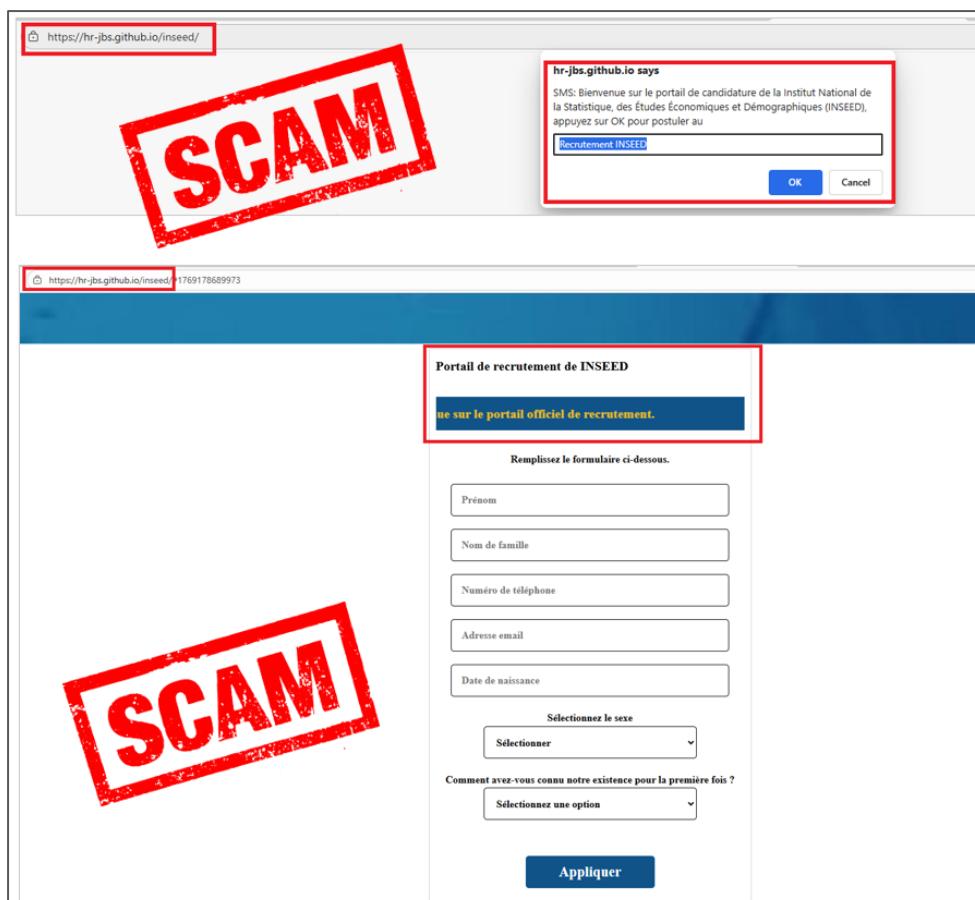


Figure 1: Page de phishing & formulaire de collecte d'informations

TLP : CLEAR