Alerte de Phishing : usurpation du site web de la CENI-TOGO

Le CERT.tg a identifié plusieurs liens malveillants vous dirigeant vers des sites web qui se présentent comme les sites officiels de la **Commission Electorale Nationale Indépendante.**
Nous avons découvert à la suite de nos investigations qu'il s'agit dans les deux cas de **site d'hameçonnage** (phishing) dont les noms de domaines principaux sont *CENI-tg.org* (IP 104.21.43.48) et applyforms.me (avec une IP qui change régulièrement).

Ci-dessous les liens malveillants :

- *hxxps://ceni-tg.applyforms.me/?m=1#1701160823571*
- *hxxps://ceni.tg.applyforms.me/?m=1#1701163078414*
- *hxxps://www.ceni-tg.org/*
  (Attention ne pas cliquer dessus)

Bien que ces sites ne soient pas une copie parfaite du site officiel, il s'agit tout de même d'un cas d'usurpation de site web, d'autant plus que la CENI **n'effectue aucun recrutement actuellement.**

L 'objectif de cette usurpation est de tromper les utilisateurs et de gagner leur confiance pour la mise en œuvre d'éventuelles fraudes plus élaborées (collecte d'informations par phishing, partage de logiciels malveillants, etc.).

Ci-dessous une capture d'écran des sites web frauduleux.

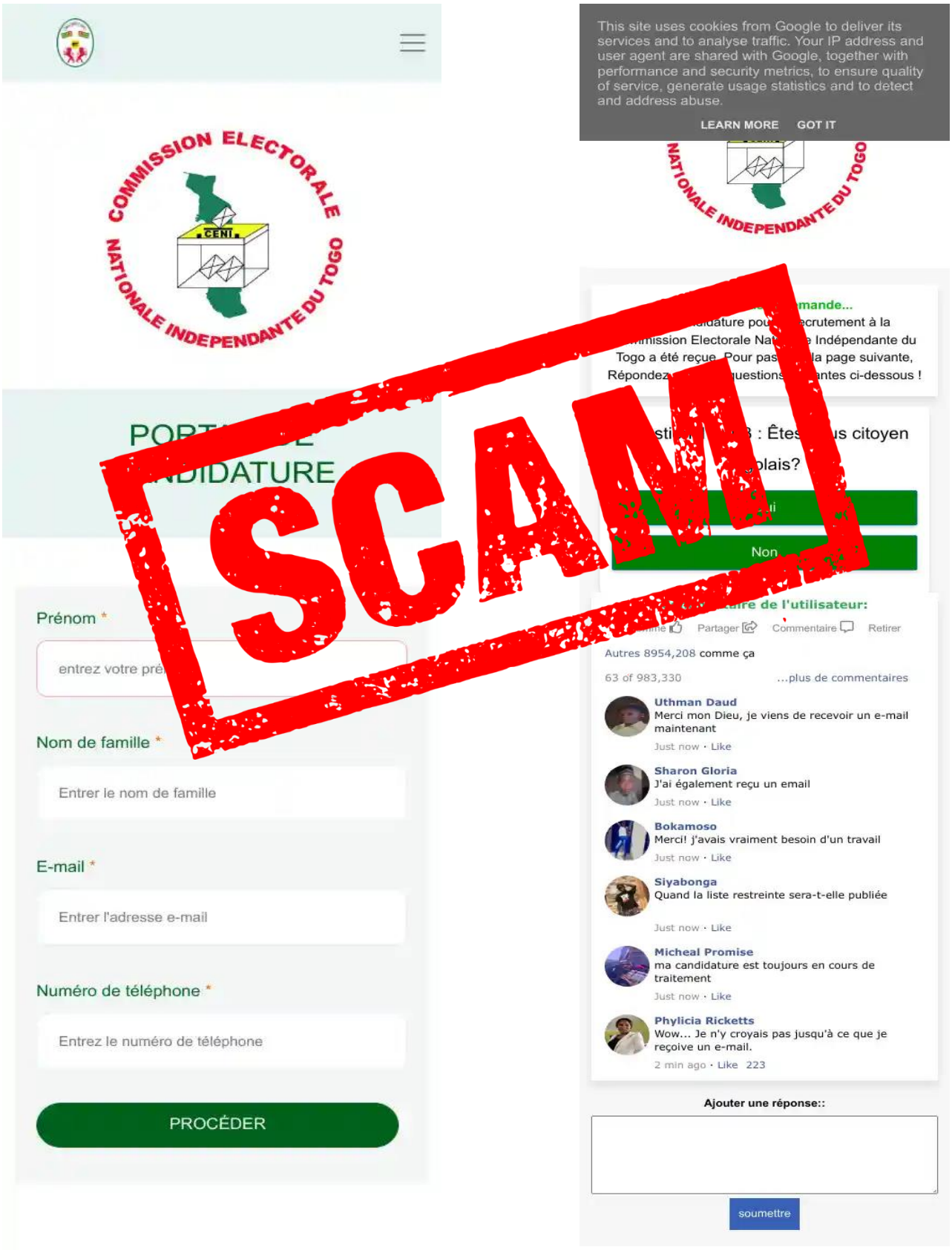

Figure 1 : sites web frauduleux

Ci-dessous une capture d'écran le site web officiel de la CENI-TOGO

Figure 2 : site web officiel de La CENI-TOGO

Comment différencier le site web officiel de la CENI TOGO au site web frauduleux ?

Le lien du site web officiel de la CENI-TOGO est le ***https://www.cenitogo.tg/*** (voir capture d'écran)

Figure 3 : Lien du site web officiel de La CENI-TOGO

Tandis que ceux des site web frauduleux sont le ***https://ceni-tg.applyforms.me*** *et* ***https://ceni.tg.applyforms.me*** (voir capture d'écran)

Figure 4 : Liens des sites web frauduleux.

Quelques mesures préventives à adopter :

Les sites de phishing sont créés pour collecter les informations personnelles des utilisateurs en vue d'utilisation malicieuse (usurpations d'identité).
Les bonnes pratiques ci-dessous à adopter vous permettrons de vous prémunir de la plupart des menaces sur internet :

- **Conseil 1** : Rester informé sur les techniques d'hameçonnage (phishing).
- **Conseil 2** : Éviter de cliquer sur des liens inconnus reçus par email ou sur les réseaux sociaux.
- **Conseil 3 :** Taper l'url du site web directement au lieu de cliquer sur les liens envoyés surtout s'il s'agit de site sensible comme les sites bancaires et commerciaux.
- **Conseil 4 :** Ne jamais donner d'informations personnelles (Nom, email, téléphone, adresses, …) ou confidentielles sur internet surtout pas sur les sites dont la source est inconnue.
- **Conseil 5** : Maintenir vos logiciels à jour : assurez-vous que vos navigateurs sont toujours à jour afin de réduire les vulnérabilités.
- **Conseil 6** : Installer des applications et logiciels officiels : assurez-vous d'installer les logiciels légitimes depuis des sources fiables mis à disposition par des magasins d'applications officiels et payer les licences adéquates lorsque le logiciel ou l'application est
  payante
- **Conseil 7** : Signaler directement sur le site du **CERT.tg** https://cert.tg/ dans la rubrique « déclarer un incident / Signaler un domaine » tout site web frauduleux ou suspect.