

## COMMUNIQUÉ DE PRESSE

Mardi 4 août 2026

### **Fausse amende par SMS : le gouvernement dévoile les résultats de son analyse technique**

Le 31 juillet 2026, le gouvernement de la Nouvelle-Calédonie, la Police nationale et l'OPT-NC alertaient conjointement la population sur une campagne de smishing usurpant l'identité de service-public.nc et de la direction des Finances publiques.

À la suite de cette alerte, le gouvernement au travers de sa direction du Numérique et de la modernisation (DINUM) a conduit une analyse technique approfondie du dispositif frauduleux. Les résultats confirment l'utilisation d'un mode opératoire sophistiqué, reposant sur des infrastructures cybercriminelles internationales.

#### **Une fraude reposant sur un écosystème criminel international**

Les investigations menées par les équipes techniques montrent que le scénario utilisé en Nouvelle-Calédonie – fausse contravention, menace de poursuites et réduction du montant en cas de paiement rapide – correspond au fonctionnement d'un kit de fraude « clé en main », commercialisé au sein de réseaux cybercriminels internationaux.

Des campagnes présentant un mode opératoire quasiment identique ont été observées ces dernières semaines dans une dizaine de pays répartis sur plusieurs continents. Selon les territoires ciblés, les fraudeurs usurpent l'identité d'administrations chargées des amendes routières, des services fiscaux, d'opérateurs de télécommunications ou encore de services de livraison.

La Nouvelle-Calédonie ne constitue donc pas une cible isolée, mais s'inscrit dans une campagne de fraude d'ampleur mondiale.

#### **Un mécanisme de vol des données bancaires en temps réel**

L'analyse révèle également que le faux site internet ne procède à aucune vérification réelle : quelle que soit la plaque d'immatriculation renseignée, un même montant d'amende fictif est systématiquement affiché.

Plus préoccupant encore, le site transmet automatiquement à un opérateur distant les premiers chiffres de la carte bancaire saisis par la victime, avant même la validation du formulaire. Cet opérateur est alors en mesure de lancer immédiatement une véritable transaction bancaire, tandis que la victime reçoit simultanément une fausse demande de code de validation (SMS ou application bancaire).

Ce procédé contourne ainsi les mécanismes habituels de double authentification, qui ne constituent plus, à eux seuls, une protection suffisante face à ce type d'escroquerie.

### **Une mobilisation technique et institutionnelle coordonnée**

Les conclusions de cette analyse ont été transmises à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dans le cadre de la coopération entre autorités compétentes en matière de cybersécurité, ainsi qu'à l'OPT-NC afin d'évaluer les possibilités de renforcement des mesures de filtrage des infrastructures réseau.

Elles contribueront également au partage d'informations avec la communauté internationale de la cybersécurité, cette campagne présentant plusieurs caractéristiques techniques qui n'avaient, à ce stade, pas encore été documentées publiquement.

### **Les recommandations demeurent inchangées**

- Ne jamais cliquer sur un lien reçu par SMS/Message annonçant une amende ou une contravention ;
- Se rendre directement sur le site officiel en saisissant l'adresse manuellement ;
- Ne jamais communiquer de coordonnées bancaires ou codes de vérification suite à un SMS/Message non sollicité ;
- En cas de saisie d'informations bancaires sur un site suspect, contacter immédiatement sa banque pour faire opposition ;
- Restez à l'écoute des alertes et préconisations techniques diffusées par le gouvernement de la Nouvelle-Calédonie ou l'OPT-NC.

### **Que faire si vous avez été victime ?**

- Contacter sans délai sa banque pour faire opposition ;
- Déposer plainte auprès de la Police nationale ou de la Gendarmerie ;
- Signaler le SMS ou le site frauduleux sur [cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) et [internet-signalement.gouv.fr](https://internet-signalement.gouv.fr)

L'infrastructure utilisée par les fraudeurs évoluant (nouveaux sites, nouveaux numéros), le gouvernement de la Nouvelle-Calédonie invite l'ensemble de la population, des administrations, des collectivités, des entreprises et des établissements publics à maintenir un niveau élevé de vigilance face à ces tentatives d'escroquerie.

\* \*  
\*