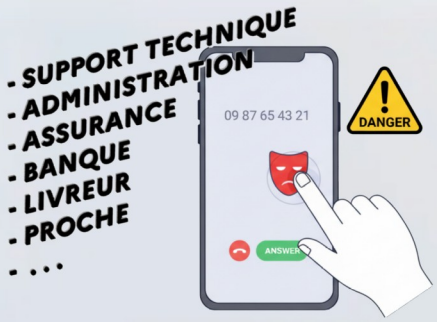
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND 80
Gendarmerie départementale de la Somme

14 novembre 2025

Le Groupement de gendarmerie départementale de la Somme alerte sur l'**arnaque au faux numéro** (ou spoofing), une **technique de fraude** sophistiquée en **pleine expansion**, reposant sur un procédé qui permet à l'appelant de changer l'**identifiant** que vous voyez s'afficher sur votre écran.

QU'EST-CE QUE L'ARNAQUE AU FAUX NUMÉRO ?



L'**arnaque au faux numéro**, ou ***spoofing***, est une technique de fraude où les escrocs affichent délibérément un **faux numéro** sur l'écran du destinataire, **masquant** ainsi leur véritable identité. Ils utilisent des logiciels ou des services en ligne pour faire croire que l'appel provient d'un **numéro légitime**, souvent celui d'une banque, d'une administration publique (impôts, Sécurité sociale), d'une entreprise de télécommunications, ou même d'un proche dont le numéro est **usurpé** pour vous **tromper**.

OBJECTIFS DES FRAUDEURS

L'objectif principal est de gagner la confiance de la victime pour l'inciter à :

- ✗ **Fournir des informations personnelles et financières** (numéros de carte bancaire, mots de passe, identifiants de connexion, codes de sécurité à usage unique) ;
- ✗ **Effectuer un transfert d'argent urgent** ;
- ✗ **Télécharger un logiciel malveillant** (malware) qui donnerait aux fraudeurs un accès à distance à l'ordinateur ou au smartphone ;
- ✗ **Valider une transaction frauduleuse** en fournissant un code reçu par SMS.

COMMENT ÇA MARCHE ?

1. **Usurpation** : L'escroc utilise un outil pour afficher un numéro de téléphone qui n'est pas le sien, choisissant souvent un numéro connu ou local pour augmenter la crédibilité.
2. **Mise en Scène** : L'appel est souvent accompagné d'un scénario de crise ou d'urgence, comme :
   « Votre compte bancaire est piraté, nous avons besoin de votre code de sécurité pour le bloquer ! »
   « Vous avez une dette aux impôts, payez immédiatement pour éviter une amende ! »
   « Nous devons procéder à une vérification technique urgente de votre ligne ! »
3. **Pression Psychologique** : Afin d'empêcher toute réflexion ou vérification, les fraudeurs instaurent un climat d'urgence et emploient un langage impératif, voire intimidant.

CONSEILS PRÉVENTIFS ESSENTIELS

Pour **déjouer** les tentatives d'usurpation d'identité (spoofing), soyez particulièrement **vigilant** aux appels et messages reçus, même provenant de sources que vous pensez **fiables** !

Si la demande est **inhabituelle** ou **suspecte**, vérifiez systématiquement son **authenticité** :

- ✔ Demandez l'**identité** de votre interlocuteur (nom/service) ;
- ✔ Rappelez-le au **numéro officiel** (en passant par le standard) pour confirmer ses demandes ;
- ✔ Demandez confirmation par un **autre canal** (email) ;
- ✔ Ne divulguez pas d'**informations** à la légère : ne communiquez **JAMAIS** vos mots de passe, codes de vérification (mot de passe à usage unique, SMS, etc), ou codes secrets par téléphone. **Aucune entité légitime** ne vous le demandera ;
- ✔ Prenez le temps : la **règle d'or** est de ne **jamais** agir sous la **pression**.