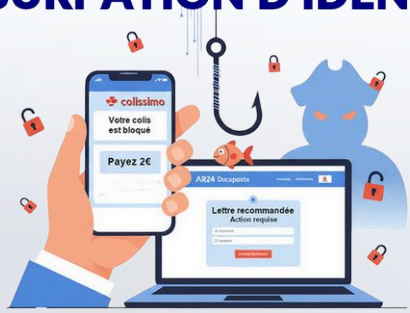
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND 80
Gendarmerie départementale de la Somme

13 octobre 2025

#RÉPONDREPRÉSENT

USURPATION D'IDENTITÉ d'une entité de confiance pour obtenir des INFORMATIONS SENSIBLES



Plusieurs **communes et entreprises de la Somme** signalent avoir été la cible de **tentatives d'hameçonnage** par des individus **usurpant l'identité** de services **légitimes** et **familiers**, comme La Poste (Colissimo) ou les solutions de recommandés électroniques comme AR24 (Docaposte).

LES DEUX TYPES DE TENTATIVES À SURVEILLER :

Type de Fraude	Le Prétexte Utilisé	L'Objectif de l'Escroc	La Règle d'Or
Faux Colissimo / Frais de livraison	Vous recevez un e-mail ou un SMS vous demandant de **payer une petite somme** (souvent 1,50 € ou 2,00 €) pour **"débloquer"** un colis soi-disant "bloqué au centre de distribution".	Vous faire cliquer sur **un lien** pour voler vos **coordonnées bancaires**.	**Ne jamais payer de frais de livraison inattendus via un lien.** Vérifiez toujours le suivi sur le site officiel de Colissimo.
Faux Recommandé Électronique (LRE)	Vous recevez une notification (parfois crédible) d'une **Lettre Recommandée Électronique** (LRE) de la part d'un service comme AR24, vous invitant à vous **identifier** pour "consulter votre courrier".	Vous faire entrer **vos identifiants** sur une fausse page pour voler vos **informations personnelles et identifiants**.	**Vérifiez l'expéditeur.** En cas de doute, accédez au site officiel par vous-même (en tapant l'adresse dans votre navigateur) pour vous connecter ou vérifier la légitimité de l'avis.

LES RÈGLES DE SÉCURITÉ À APPLIQUER :

1. **Vérifiez l'adresse de l'expéditeur :** Les e-mails de phishing utilisent souvent des adresses qui semblent légitimes mais comportent des erreurs (fautes d'orthographe, extension inhabituelle, etc.).
2. **Méfiez-vous de l'urgence :** Les messages frauduleux contiennent souvent des formulations qui incitent à l'action immédiate ("Paiement immédiat", "Dernier avertissement"). Prenez le temps de de la réflexion.
3. **Ne cliquez pas sur les liens suspects :** En cas de doute, ne cliquez pas. Préférez toujours vous rendre sur le site officiel par vous-même pour vous connecter ou vérifier l'information.
4. **Ne communiquez jamais d'informations sensibles :** Aucune organisation légitime ne vous demandera vos mots de passe ou l'intégralité de vos coordonnées bancaires par e-mail ou SMS.

Votre vigilance est votre première et plus importante ligne de défense contre la cybercriminalité : les escrocs contournent les systèmes de sécurité en misant sur l'erreur humaine. L'hameçonnage cible l'individu en jouant sur l'urgence, la curiosité ou la peur pour obtenir un clic ou une information.

En appliquant rigoureusement les règles de sécurité (vérification de l'expéditeur, méfiance face aux demandes urgentes et accès direct aux sites officiels), vous protégez efficacement vos données et celles de votre structure professionnelle.