



## L'ARNAQUE AU FAUX RIB

*Quand les fraudeurs piratent  
VOS PRESTATAIRES pour  
détourner VOS PAIEMENTS*



Un **établissement scolaire** de la Somme a récemment été victime d'une fraude financière sophistiquée après la compromission de la messagerie de l'un de ses **prestataires**. Le préjudice est évalué à plus de **15 000 euros**.

Le mode opératoire, étape par étape :

- 1. Piratage :** Les cybercriminels prennent le contrôle de la boîte mail d'un partenaire légitime (via un mot de passe faible ou une campagne d'hameçonnage).
- 2. Espionnage & Interception :** Ils analysent les échanges et volent de vraies factures en attente de règlement.
- 3. Falsification :** Les pirates modifient le RIB sur les documents originaux.
- 4. Envoi :** Depuis la vraie adresse du fournisseur, ils réclament le paiement des factures vers le nouveau compte bancaire frauduleux. L'email, légitime en apparence, déjoue les filtres de sécurité.

Ces deux types d'atteintes (piratage de messagerie et escroquerie au faux RIB) sont susceptibles de frapper n'importe quelle structure !

**ENTREPRISES, COLLECTIVITÉS, ASSOCIATIONS, PARTICULIERS,**  
*les conseils de prévention suivants vous concernent tous :*

<b>POUR L'ENTITÉ DÉBITRICE</b> Cible de la fausse facture	<b>POUR L'ENTITÉ CRÉANCIÈRE</b> Victime du piratage de messagerie
<ul style="list-style-type: none"> <li>› <b>VÉRIFICATION CROISÉE :</b> Confirmez systématiquement tout changement de RIB par téléphone, en utilisant un numéro déjà connu.</li> <li>› <b>CONTRÔLE INTERNE :</b> Formez les équipes à repérer les signaux d'alerte (urgence inhabituelle, modification de dernière minute) et imposez une double validation pour les gros virements.</li> </ul>	<ul style="list-style-type: none"> <li>› <b>MOTS DE PASSE :</b> Sécurisez les messageries avec des codes complexes et uniques.</li> <li>› <b>DOUBLE AUTHENTIFICATION (2FA) :</b> Activez-la systématiquement pour bloquer les accès frauduleux.</li> </ul>

