MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

15 mai 2025

ALERTECYBERGEND

Ce jour, une commune du département nous a signalé avoir reçu un courriel frauduleux. Ce message, soi-disant envoyé par une entreprise partenaire, contenait une facture et un nouveau RIB. Fort heureusement, la commune a fait preuve de vigilance en contactant l'entreprise, laquelle a confirmé ne pas être l'expéditeur et que le RIB était inconnu.

Grâce à cette prudence, la tentative d'escroquerie a été déjouée.

Dans ce type de fraude, le **but** de l'escroc est de **duper sa cible** en se faisant passer pour un créancier légitime (comme un fournisseur, un client, un notaire, un avocat, un propriétaire ou un bailleur). L'**objectif** est d'inciter la victime à effectuer un **virement** vers un compte bancaire contrôlé par l'imposteur. Cette **escroquerie** fait souvent suite au **piratage** d'une **boîte de messagerie**, qu'il s'agisse de celle du créancier avec lequel la victime communique habituellement, ou de celle de la victime elle-même, dont l'accès a été compromis par le fraudeur.

COMMENT SE PROTÉGER DES ESCROQUERIES « AU FAUX RIB » ?

- **Vérifiez systématiquement** toute modification de coordonnées bancaires. En cas de réception d'un nouveau RIB, contactez votre fournisseur, client, ou autre partenaire habituel par un canal de communication que vous utilisez habituellement (par téléphone, par exemple) pour confirmer le changement. **Ne vous fiez pas uniquement aux informations contenues dans l'e-mail ou le courrier**.

- Soyez vigilant quant à l'**adresse e-mail de l'expéditeur**. Examinez attentivement l'adresse e-mail. Des différences subtiles (fautes d'orthographe, caractères ajoutés ou inversés) peuvent indiquer une tentative de fraude.

- **Méfiez-vous** des demandes de changement de RIB, et notamment celles **urgentes** ou **inhabituelles**.

- **Sécurisez** vos propres systèmes d'information :
  > Utilisez des **mots de passe** complexes et différents pour vos comptes en ligne.
  > Activez l'**authentification à double facteur** (2FA) lorsque cela est possible, notamment pour votre messagerie électronique et vos comptes bancaires.
  > **Maintenez vos logiciels** (système d'exploitation, antivirus, etc.) **à jour** pour vous protéger contre les vulnérabilités connues.
  > **Sensibilisez vos employés** aux risques de phishing et d'escroqueries en ligne.

- Établissez des **procédures de contrôle interne strictes** pour les paiements.

- **Ne cliquez pas** sur des liens ou n'ouvrez pas de pièces jointes provenant d'expéditeurs inconnus ou suspects.

- En cas de doute, **contactez directement votre banque**. Elle pourra vous conseiller et vous informer sur les éventuelles tentatives de fraude.

EN ADOPTANT CES RÉFLEXES ET EN RESTANT VIGILANT, VOUS RÉDUIREZ CONSIDÉRABLEMENT LES RISQUES DE TOMBER DANS LE PIÈGE DE L'ESCROQUERIE AU FAUX RIB.