MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

**Groupement de gendarmerie départementale de la Somme**

*16 octobre 2024*

# ALERTECYBERGEND

**Début octobre, une entreprise de la Somme a été la cible d'une escroquerie dite « au virement » ou « au faux RIB ». Le pirate a ainsi déterminé l'entreprise à lui faire un virement, en usurpant l'identité de son créancier. Le préjudice subi s'élève à plus de 195 000 euros.**

Dans ce type d'arnaque, l'escroc a pour objectif de tromper la victime, en usurpant l'identité d'un créancier avec lequel elle est en relation (fournisseur, client, notaire, avocat, propriétaire/bailleur…), afin de lui faire réaliser un virement vers un compte bancaire détenu et contrôlé par l'usurpateur. Cette escroquerie est souvent consécutive au piratage d'un compte de messagerie (mail) : il peut s'agir du compte du créancier avec lequel la victime est en relation ou bien de celui de la victime dont l'escroc aura pris le contrôle.

Dans le cas présent, le fraudeur a utilisé des techniques sophistiquées d'ingénierie sociale et d'hameçonnage (phishing) pour tromper les collaborateurs de l'entreprise et obtenir leur confiance. En l'occurrence, il a employé un e-mail falsifié imitant à la perfection la communication habituelle avec le fournisseur et a obtenu le changement de coordonnées bancaires en contactant l'entreprise pour lui demander d'enregistrer un nouveau RIB.

L'entreprise victime disposait pourtant d'un processus censé vérifier l'authenticité des demandes de modification de coordonnées bancaires. Ce protocole, bien que théoriquement robuste, n'a pas été appliqué avec la rigueur nécessaire, laissant ainsi une porte ouverte. Cette défaillance a eu des conséquences significatives, puisque l'entreprise a indument transmis la somme de 195 899 euros au fraudeur. De plus, le délai écoulé entre la commission de l'escroquerie et sa découverte a rendu impossible la récupération des fonds détournés.

## COMMENT SE PROTÉGER DES ARNAQUES « AU VIREMENT » OU « AU FAUX RIB » ?

- **Sensibilisez** vos collaborateurs ;
- **Contactez directement votre créancier** pour toute demande de virement sur un nouveau RIB reçu par message : appelez l'intéressé sur le numéro que vous utilisez habituellement pour lui faire confirmer le message et les coordonnées du RIB reçus ;
- **Méfiez-vous des messages** qui vous incitent à communiquer votre mot de passe de messagerie ou toute autre information sensible ;
- **Utilisez des mots de passe différents et complexes** pour chaque site et application que vous utilisez. Activez la double authentification quand elle est disponible ;
- Appliquez de manière régulière et systématique les **mises à jour de sécurité** ;
- N'installez des applications ou logiciels que depuis les **sites ou magasins officiels** ;
- Utilisez un **antivirus**.

## QUE FAIRE SI VOUS ÊTES VICTIME ?

- ✔ Alertez immédiatement votre **banque** de l'opération frauduleuse ;
- ✔ Alertez au plus vite le **créancier** dont l'identité a été usurpée ;
- ✔ Conservez les **preuves**, notamment les messages reçus (mails, SMS,…), les relevés de comptes, les factures ou toute autre information qui pourront vous servir pour signaler les faits ;
- ✔ Vérifiez les **paramètres** de votre messagerie : assurez-vous de l'absence de redirection ou de règles de filtrage et, si vous en identifiez, faites des photos ou des captures d'écran avant de les supprimer ;
- ✔ **Changez immédiatement votre mot de passe**, si l'escroquerie a pu être réalisée suite au piratage de votre messagerie ;
- ✔ Déposez **plainte**.