

#4 Sécurité Numérique

Publié le 19 août 2019 – Mis à jour le 28 novembre 2019



Date(s)

le 19 août 2019

Des cas d'escroqueries ont déjà été rencontrés par des ordinateurs et des comptables publics. Certaines fraudes ont été déjouées grâce à la vigilance des agents, mais d'autres n'ont pu être évitées.

**FACE AUX TENTATIVES
D'ESCROQUERIE, SOYONS PLUS
VIGILANTS !**

QUI EST CONCERNÉ ?

Réalisée par téléphone ou par courriel, l'escroquerie aux faux ordres de virement concerne les entreprises de toute taille de tous les secteurs ainsi que l'état, les établissements publics nationaux, les collectivités et établissements publics locaux ou les établissements publics de santé.

DE QUOI S'AGIT-IL ?

Il existe deux grands types d'escroquerie :

La "fraude au président"

Les escrocs demandent d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre de la hiérarchie, sous prétexte d'une facture à régler, de provision de contrat ou autres.

Ils peuvent également se faire passer pour l'éditeur de logiciel de comptabilité, un responsable informatique souhaitant réaliser des tests à distance et réaliser des opérations frauduleuses sur le poste de l'agent.

Le "Changement de RIB" via usurpation d'identité

Les fraudeurs envoient un courrier ou téléphonent à un agent des services de l'ordonnateur ou du comptable en se faisant passer pour un fournisseur ou une société d'affacturage.

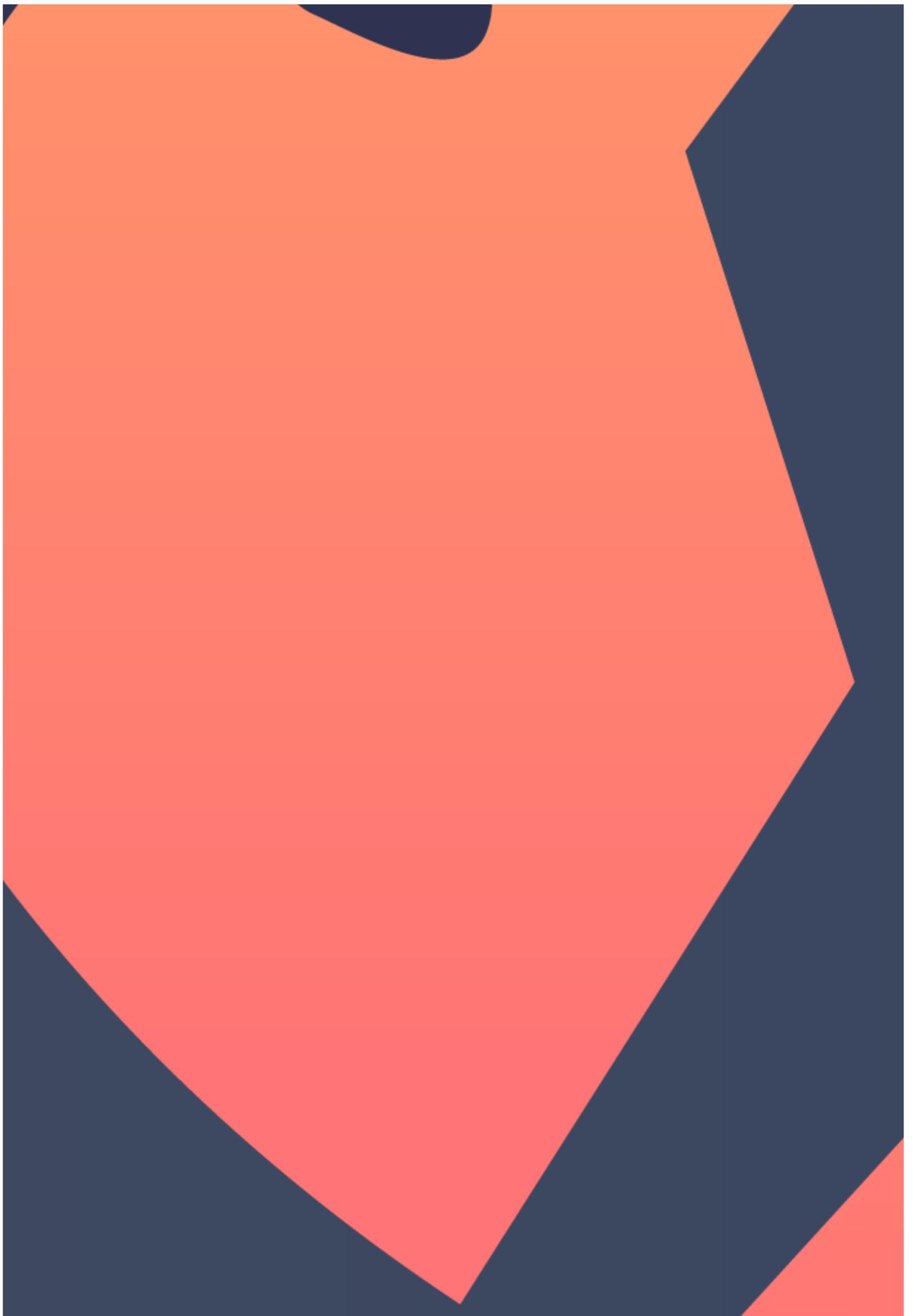
Ils lui demandent de diriger désormais ses versements vers un autre compte bancaire, le plus souvent domicilié à l'étranger.

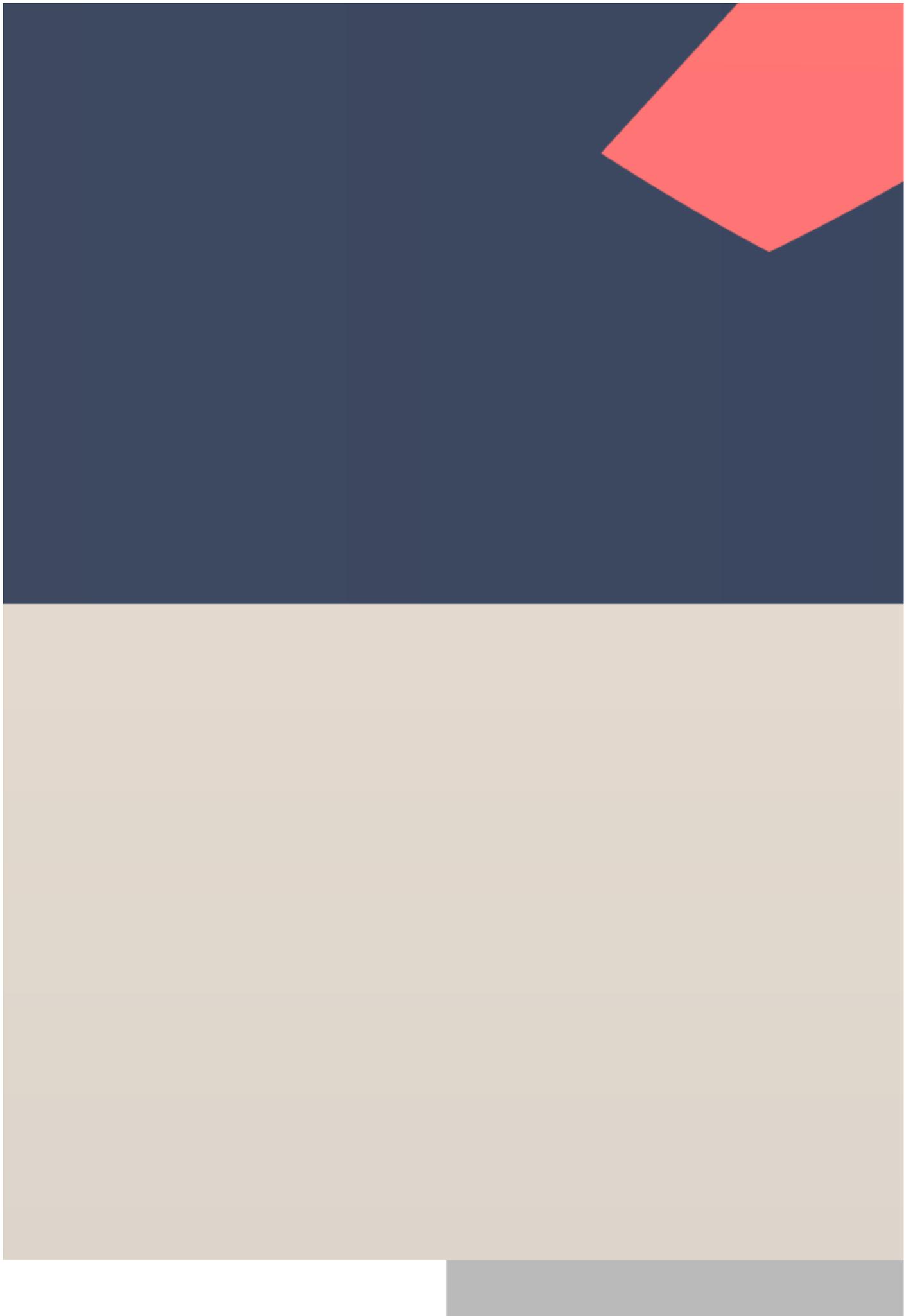
COMMENT SE PRÉMUNIR DE L'ESCROQUERIE ?

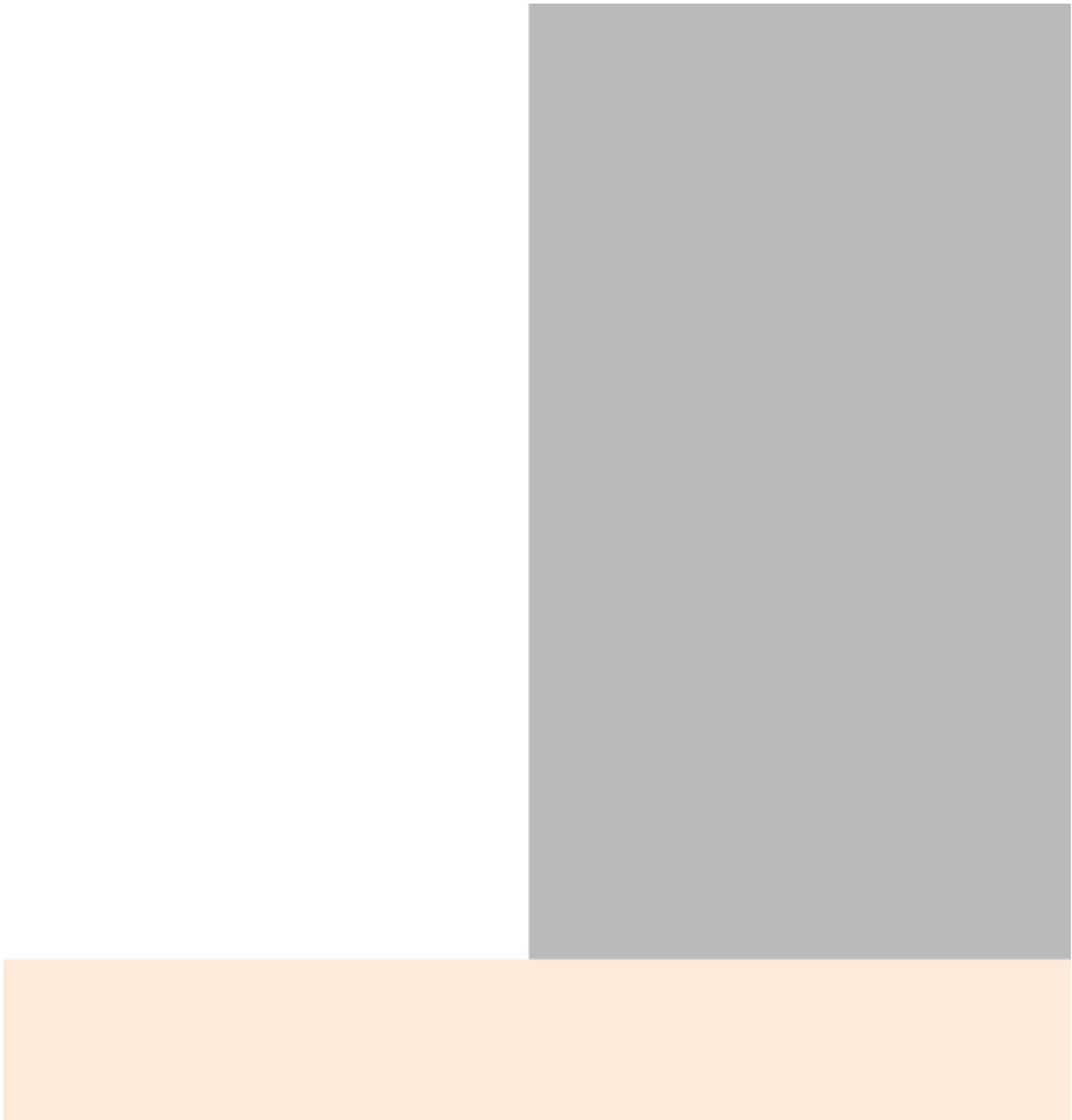
- **Ne pas divulguer à l'extérieur, ou à un contact inconnu, d'informations** concernant l'administration et ses fournisseurs (organisation, employés, procédures...)
- **Avoir un usage prudent des réseaux sociaux** privés et professionnels.
- **Informer/sensibiliser** régulièrement l'ensemble des agents des services financiers.

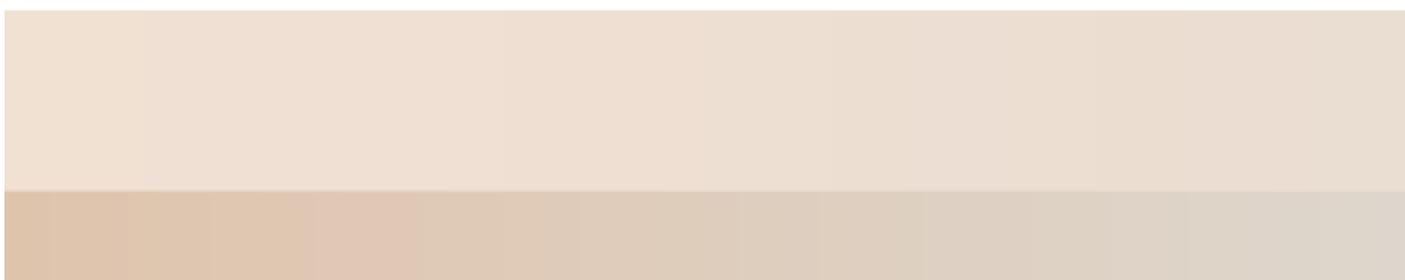












COMMENT DÉJOUER LA FRAUDE ?

- **L'agent ne doit pas céder à la pression de l'interlocuteur souhaitant un paiement rapide.** Au moindre doute, **il faut se référer immédiatement à sa hiérarchie;**
- Il faut porter un regard critique sur les demandes urgentes ou la transmission de nouvelles coordonnées à tous les niveaux de la chaîne de la dépense;
- Il ne faut pas hésiter à contacter son interlocuteur habituel avec les coordonnées déjà connues de la société ou recherchées sur un annuaire officiel.

- Il faut rompre la chaîne pour les courriers douteux en saisissant soi-même l'adresse habituelle du donneur d'ordre, voire en le contactant directement à son numéro de téléphone usuel.

COMMENT RECONNAÎTRE UNE ESCROQUERIE ?

La demande écrite ou orale de l'escroc comporte plusieurs incohérences de noms, de prénoms, d'adresse de messagerie !

**SAVEZ-VOUS RECONNAÎTRE UN MAIL FRAUDULEUX ? [LIRE L'ARTICLE.](#)(
/SECURITE-NUMERIQUE/2-SECURITE-NUMERIQUE-25599.KJSP?
RH=1484733902939)**

[https://dsi.uca.fr/actualites/4-securite-numerique\(https://dsi.uca.fr/actualites/4-securite-numerique\)](https://dsi.uca.fr/actualites/4-securite-numerique(https://dsi.uca.fr/actualites/4-securite-numerique))