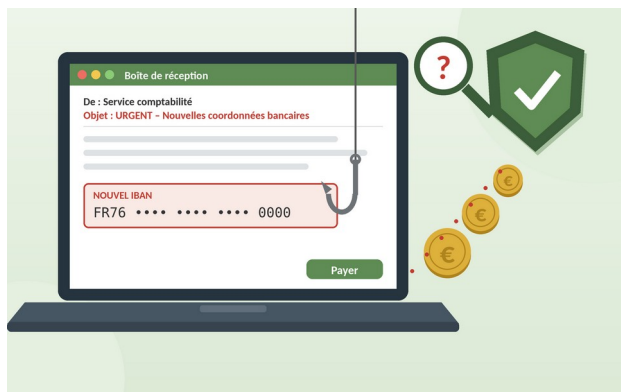


CYBERMOIS 2026 – SEMAINE 3

# Faux RIB, faux fournisseur : vérifiez avant de payer



Note de sensibilisation – Green Earth Digital

Un simple mail suffit à détourner un paiement. Pas besoin de pirater vos systèmes : le fraudeur s'attaque à vos habitudes et à vos procédures. Grandes entreprises, PME, associations ou collectivités : toutes les structures qui paient des fournisseurs sont concernées.

## Un scénario bien rodé

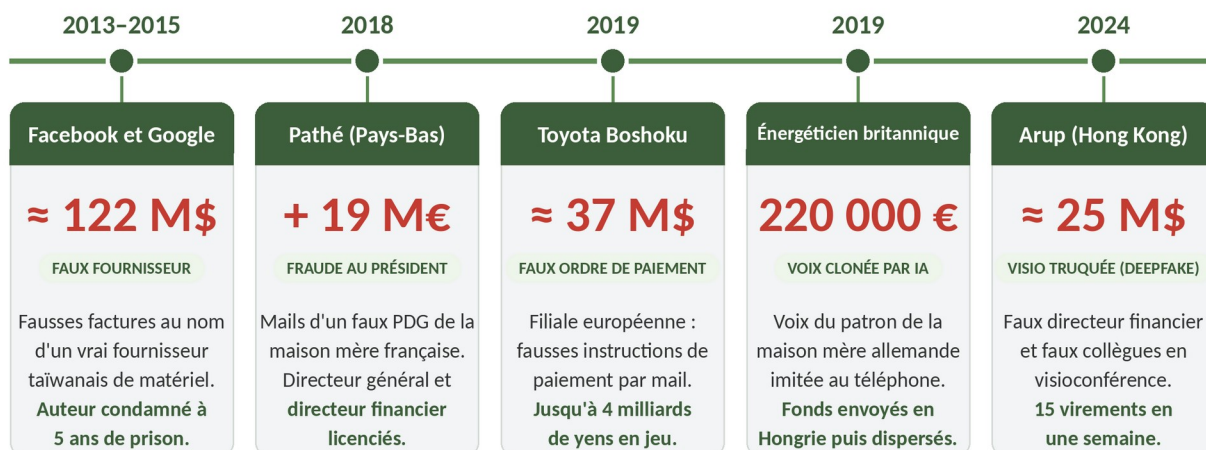
Un matin, la comptabilité reçoit un mail d'un fournisseur habituel : « Suite à un changement de banque, merci d'utiliser désormais nos nouvelles coordonnées bancaires. » Le ton est correct, la signature est la bonne, la facture est conforme. Le virement part. Quelques semaines plus tard, le vrai fournisseur relance pour une facture impayée. L'argent, lui, est déjà loin.

|   |                           |                                                                                                                                                         |
|---|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <b>Repérage</b>           | Le fraudeur collecte des informations : fournisseurs, interlocuteurs, organigramme, factures en cours (sites web, réseaux sociaux, messagerie piratée). |
| 2 | <b>Usurpation</b>         | Il écrit depuis une adresse presque identique, ou depuis la vraie boîte mail du fournisseur, piratée.                                                   |
| 3 | <b>Prétexte</b>           | Changement de banque, audit, opération confidentielle, urgence de fin de mois...                                                                        |
| 4 | <b>Virement</b>           | Le paiement est effectué sur un compte contrôlé par le fraudeur.                                                                                        |
| 5 | <b>Découverte tardive</b> | La fraude n'apparaît qu'à la relance du vrai fournisseur, souvent trop tard pour récupérer les fonds.                                                   |

**Le fraudeur n'attaque pas votre système informatique : il attaque vos procédures.**

## 01 DES CAS BIEN RÉELS

Multinationales, groupes industriels ou PME : aucune structure n'est à l'abri. Quelques affaires parmi les plus marquantes, toutes rendues publiques :



Le point commun de ces affaires : aucun système informatique « piraté » au sens classique. À chaque fois, c'est une personne de bonne foi qui a validé le paiement, convaincue d'agir pour son entreprise.

## 02 L'AMPLEUR DU PHÉNOMÈNE EN CHIFFRES

Dans le monde



En France

Baromètre Allianz Trade / Odoxa, sept. 2026



En France, la menace touche particulièrement les structures de taille moyenne : 60 % des PME et 85 % des ETI et grandes entreprises déclarent avoir été visées. 76 % des dirigeants estiment que l'intelligence artificielle augmente le risque de fraude.

### 03 LES CONSÉQUENCES : BIEN AU-DELÀ DE LA PERTE FINANCIÈRE

Un faux virement ne se résume pas à une ligne dans les comptes. Ses effets se font sentir longtemps, et à tous les niveaux de l'entreprise :

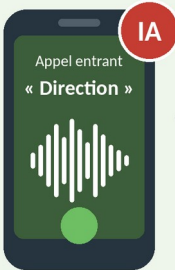
|                                            |                                                                                                                                               |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Perte financière souvent définitive</b> | Les fonds sont transférés en cascade vers plusieurs comptes et pays en quelques heures. Passé ce délai, ils sont rarement récupérés.          |
| <b>Trésorerie fragilisée</b>               | Pour une PME, un seul virement détourné peut absorber des mois de marge et mettre en difficulté le paiement des salaires ou des fournisseurs. |
| <b>Double paiement</b>                     | Le vrai fournisseur n'a rien reçu : la facture reste due et doit être payée une seconde fois.                                                 |
| <b>Responsabilités internes</b>            | Recherche des responsabilités, sanctions, voire licenciements : chez Pathé, le directeur général et le directeur financier ont été licenciés. |
| <b>Relations commerciales</b>              | Perte de confiance entre clients et fournisseurs, litiges sur la responsabilité, contrats remis en question.                                  |
| <b>Assurance</b>                           | La prise en charge n'est pas automatique : elle dépend du contrat (fraude, cyber) et des procédures de contrôle en place.                     |
| <b>Temps, image et facteur humain</b>      | Plainte, enquête, échanges avec la banque et les assureurs ; atteinte à la réputation ; collaborateur victime durablement affecté.            |

**Le coût réel d'une fraude dépasse presque toujours le montant du virement détourné.**

## 04 LES PRINCIPALES VARIANTES

| Fraude                                        | Comment elle se présente                                                                                          |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Faux fournisseur / faux RIB</b>            | Un fournisseur connu annonce un changement de coordonnées bancaires avant une échéance de paiement.               |
| <b>Fraude au président</b>                    | Un pseudo-dirigeant demande un virement urgent et confidentiel, en dehors des circuits habituels.                 |
| <b>Faux salarié</b>                           | Un « collaborateur » demande par mail la modification du RIB sur lequel est versé son salaire.                    |
| <b>Faux conseiller bancaire ou technicien</b> | Un appel demande de valider une opération, de communiquer un code ou d'installer un logiciel d'assistance.        |
| <b>Usurpation assistée par IA</b>             | Mails sans faute, voix imitée au téléphone, voire visioconférence truquée : les signaux classiques disparaissent. |

### Zoom : la fraude au président à l'heure de l'intelligence artificielle



Appel entrant  
« Direction »

« C'est moi. Je suis en réunion, j'ai besoin d'un virement urgent. Pas un mot à personne pour l'instant. »

**Une voix familière... générée par intelligence artificielle.**

Quelques secondes d'enregistrement (vidéo, message vocal) peuvent suffire à imiter une voix.

**LE BON RÉFLEXE**

Raccrocher, puis rappeler la personne sur son **numéro habituel**.

Convenir d'un mot de passe ou d'une question de contrôle en interne.

### Pourquoi ça marche ?

Ces fraudes ne reposent pas sur la technique, mais sur des ressorts humains que chacun peut reconnaître :

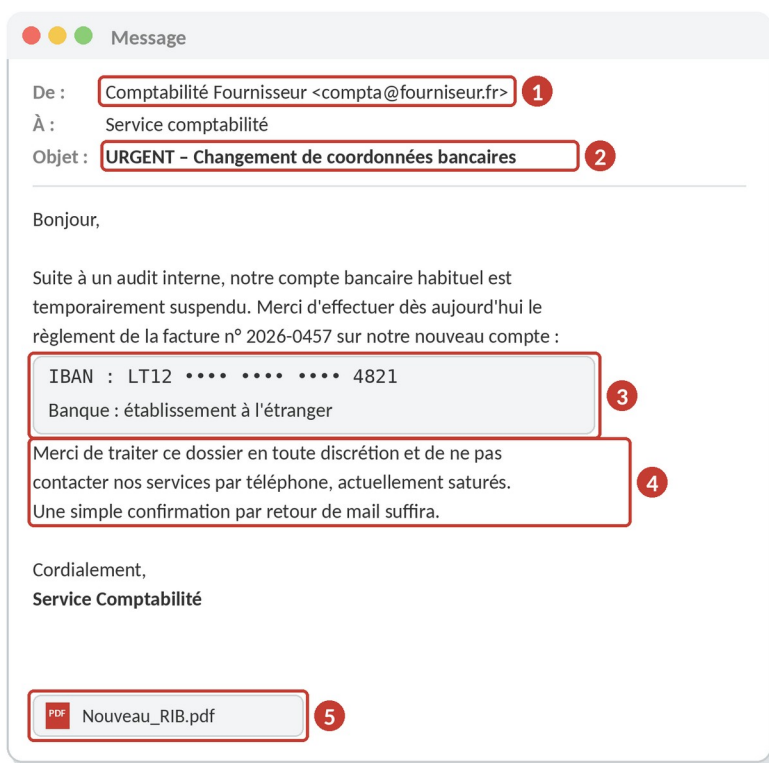
|                     |                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------|
| <b>L'autorité</b>   | Une demande qui semble venir de la direction ou d'un partenaire important est rarement remise en question. |
| <b>L'urgence</b>    | Une échéance, une pénalité, une opération « à boucler aujourd'hui » : plus de temps pour vérifier.         |
| <b>La routine</b>   | Le fournisseur est connu, la facture est attendue : le paiement paraît normal.                             |
| <b>La confiance</b> | Le message reprend les bons noms, les bons montants et le bon ton, grâce aux informations collectées.      |

## 05 LES SIGNAUX D'ALERTE



Un seul signal suffit à déclencher une vérification.

### Exemple de mail frauduleux : saurez-vous repérer les pièges ?



#### Les pièges à repérer

- 1 Adresse presque identique**  
« fournisseur » : il manque un « s ».
- 2 Urgence affichée**  
« URGENT », « dès aujourd'hui » : pour vous empêcher de vérifier.
- 3 Nouveau compte inhabituel**  
Banque différente, souvent à l'étranger.
- 4 Discretion et pas d'appel**  
Le fraudeur bloque le seul moyen de le démasquer.
- 5 RIB en pièce jointe**  
Un document se falsifie facilement.

**Le bon réflexe :**  
rappeler le fournisseur sur un numéro déjà connu.

### Attention aux adresses qui se ressemblent : un caractère suffit à changer d'expéditeur.

| Adresse habituelle    | Adresse frauduleuse       | Ce qui change          |
|-----------------------|---------------------------|------------------------|
| compta@fournisseur.fr | compta@fourniseur.fr      | Une lettre en moins    |
| compta@fournisseur.fr | compta@fournisseur-fr.com | Domaine différent      |
| compta@fournisseur.fr | compta@fournlisseur.fr    | Le « i » devient « l » |

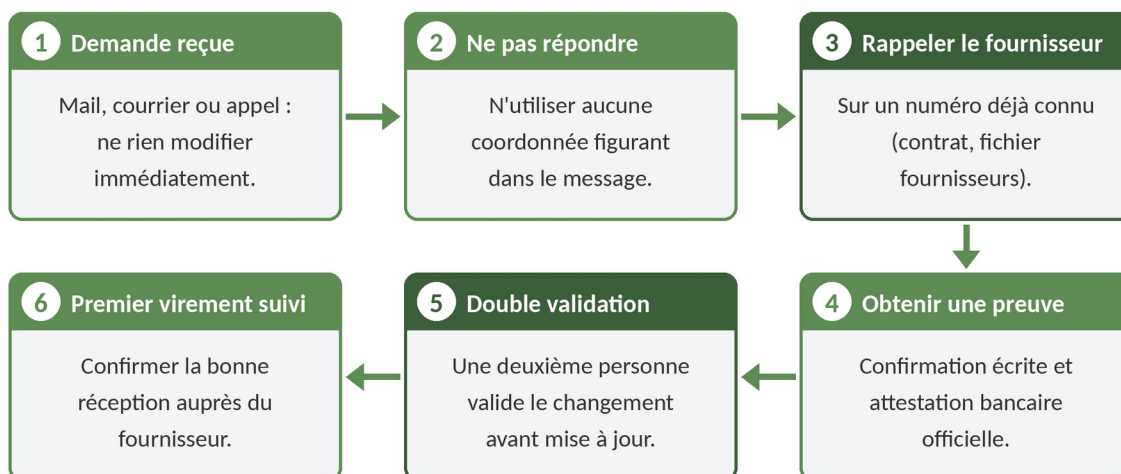
Exemples fictifs. Lorsque la vraie messagerie du fournisseur est piratée, l'adresse est exacte : seule une vérification par un autre canal permet de détecter la fraude.

## 06 LES BONS RÉFLEXES

|                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>AVANT CHAQUE PAIEMENT</b></p> <ul style="list-style-type: none"> <li>✓ Vérifier tout changement de RIB par un autre canal.</li> <li>✓ Se méfier de l'urgence et de la confidentialité.</li> <li>✓ Comparer avec l'historique du fournisseur.</li> <li>✓ Ne jamais valider sous la pression.</li> </ul> | <p><b>SUR LA MESSAGERIE</b></p> <ul style="list-style-type: none"> <li>✓ Activer la double authentification.</li> <li>✓ Vérifier l'adresse réelle de l'expéditeur.</li> <li>✓ Contrôler les règles de transfert automatique.</li> <li>✓ Signaler les mails suspects.</li> </ul>          |
| <p><b>DANS L'ORGANISATION</b></p> <ul style="list-style-type: none"> <li>✓ Écrire une procédure de changement de RIB.</li> <li>✓ Séparer saisie et validation des paiements.</li> <li>✓ Tenir un fichier fournisseurs de référence.</li> <li>✓ Limiter les informations publiées en ligne.</li> </ul>        | <p><b>AVEC LES ÉQUIPES</b></p> <ul style="list-style-type: none"> <li>✓ Sensibiliser comptabilité, achats et assistants.</li> <li>✓ Autoriser chacun à dire « je vérifie ».</li> <li>✓ Partager les tentatives détectées.</li> <li>✓ Inclure les remplaçants et intérimaires.</li> </ul> |

## 07 LA PROCÉDURE DE VÉRIFICATION D'UN CHANGEMENT DE RIB

Six étapes simples, à formaliser par écrit et à appliquer sans exception, quel que soit l'interlocuteur :



**! Un doute ? Bloquer le paiement et alerter la direction.**

## 08 LA FRAUDE A EU LIEU : AGIR SANS ATTENDRE

|   |                         |                                                                                                                                           |
|---|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Appeler la banque       | Immédiatement, pour demander le blocage ou le rappel des fonds.                                                                           |
| 2 | Alerter la direction    | Et le vrai fournisseur, dont la messagerie est peut-être compromise.                                                                      |
| 3 | Conserver les preuves   | Mails (avec leurs en-têtes), factures, ordres de virement, échanges téléphoniques.                                                        |
| 4 | Sécuriser la messagerie | Changer les mots de passe, vérifier les règles de transfert et les connexions.                                                            |
| 5 | Porter plainte          | Et signaler la fraude aux autorités compétentes (en France : <a href="https://cybermalveillance.gouv.fr">cybermalveillance.gouv.fr</a> ). |
| 6 | Tirer les leçons        | Analyser la faille et renforcer la procédure pour éviter qu'elle ne se reproduise.                                                        |

**Chaque heure compte : plus l'alerte est rapide, plus les chances de récupérer les fonds sont grandes.**

### Après la fraude : chercher la cause, pas un coupable

La personne qui a validé le virement est d'abord une victime : elle a été manipulée par des professionnels. Désigner un coupable n'empêche pas la fraude suivante et produit l'effet inverse de celui recherché : si les équipes craignent d'être sanctionnées, elles hésitent à signaler un doute ou une erreur, alors que les premières heures sont décisives. L'approche à privilégier est celle de la « culture juste », issue de la sécurité industrielle : distinguer les situations, puis traiter les causes.

|                             |                                                                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erreur de bonne foi         | La personne a été trompée malgré les procédures, ou faute de procédure : accompagnement, formation, renforcement de l'organisation.                         |
| Procédure connue contournée | Les consignes existaient et ont été volontairement ignorées : mesure managériale proportionnée, après analyse du contexte (pression, charge de travail...). |
| Complicité ou malveillance  | Cas exceptionnel : procédure disciplinaire et judiciaire.                                                                                                   |

Une fois l'urgence traitée, l'analyse des causes racines (méthode des 5 pourquoi, arbre des causes) permet d'identifier la vraie faille : absence de procédure de vérification, validation par une seule personne, messagerie mal protégée, pression des délais... Les actions correctives et le retour d'expérience partagé avec les équipes transforment l'incident en progrès collectif.

**Un collaborateur qui ose alerter vite vaut mieux qu'un collaborateur qui a peur de parler.**

## 09 AUTO-DIAGNOSTIC : SIX QUESTIONS À SE POSER

|   |                                                                                      |                                                           |
|---|--------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 1 | Disposez-vous d'une procédure écrite de changement de RIB ?                          | Oui <input type="checkbox"/> Non <input type="checkbox"/> |
| 2 | Les changements de coordonnées sont-ils vérifiés par un rappel sur un numéro connu ? | Oui <input type="checkbox"/> Non <input type="checkbox"/> |
| 3 | Les paiements importants sont-ils validés par deux personnes ?                       | Oui <input type="checkbox"/> Non <input type="checkbox"/> |
| 4 | La double authentification est-elle activée sur les messageries ?                    | Oui <input type="checkbox"/> Non <input type="checkbox"/> |
| 5 | Vos équipes comptables et achats ont-elles été sensibilisées ?                       | Oui <input type="checkbox"/> Non <input type="checkbox"/> |
| 6 | Savez-vous qui appeler, et dans quel ordre, en cas de fraude ?                       | Oui <input type="checkbox"/> Non <input type="checkbox"/> |

## L'ACCOMPAGNEMENT DE GREEN EARTH DIGITAL

Green Earth Digital accompagne les entreprises vers des environnements plus performants, connectés, sécurisés et durables. Face à la fraude au paiement, nous intervenons notamment pour :

|                                     |                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Sensibilisation</b>              | Ateliers pratiques pour les équipes comptables, achats, assistants et managers, à partir de cas réels. |
| <b>Sécurisation des messageries</b> | Double authentification, protection contre l'usurpation d'adresse, contrôle des règles de transfert.   |
| <b>Revue des procédures</b>         | Analyse du circuit fournisseurs et paiements, séparation des tâches, procédure de changement de RIB.   |
| <b>Exercices et simulations</b>     | Campagnes de faux mails et mises en situation pour tester les réflexes.                                |
| <b>Approche QSE</b>                 | Intégration des procédures dans le système de management et suivi dans le temps.                       |

### VÉRIFIER • DOUBLE VALIDER • SÉCURISER • SIGNALER

*Parce qu'un seul virement peut coûter très cher.*

#### Green Earth Digital

Performance • Connectivité • Sécurité • Durabilité

Pour échanger sur vos enjeux : [info@greeneearth-digital.fr](mailto:info@greeneearth-digital.fr) / [sales@greeneearth-digital.fr](mailto:sales@greeneearth-digital.fr)

Sources : FBI – Internet Crime Complaint Center (IC3), rapport 2024 ; baromètre Allianz Trade / Odoxa, septembre 2026 ; communications des entreprises et presse internationale (Fortune, BleepingComputer, Sophos, The Next Web, Accountant.nl).