# LE POINT SUR...

## Fraude assistée par l'IA

*Faux ordres de virement, usurpation de dirigeants et de fournisseurs*

La fraude au virement figure désormais parmi les trois principales menaces signalées par les entreprises et les associations, avec des demandes d'assistance en hausse de 93 % en un an. Le procédé n'est pas nouveau, mais l'intelligence artificielle a supprimé les signaux qui permettaient jusqu'ici de l'identifier : voix clonée, visioconférence truquée, courriel sans défaut. Toutes les tailles d'entreprise sont concernées, y compris les plus petites. Les parades relèvent de l'organisation interne bien davantage que de la technique.

### Ce qu'il faut comprendre

Le scénario est constant : un tiers se fait passer pour le dirigeant, pour un conseiller bancaire ou pour un fournisseur habituel, et obtient un virement ou une modification de coordonnées bancaires. Ce qui a changé tient à la qualité de l'imitation. Un clonage vocal - une voix reconstituée par une IA - s'obtient à partir de quelques secondes d'enregistrement public : vidéo de présentation, interview, message d'accueil téléphonique. Une fausse visioconférence se prépare en une demi-journée.

Deux conséquences en découlent. Les repères habituels ne fonctionnent plus : le courriel mal rédigé, l'accent qui sonne faux, le contre-appel rassurant. Et le coût d'une attaque, tombé à quelques dizaines d'euros, rend une entreprise de vingt salariés aussi rentable à viser qu'un grand groupe.

Un troisième mécanisme explique la précision de ces demandes : dans de nombreux cas, le fraudeur a d'abord pénétré une boîte de messagerie - celle de l'entreprise ou celle d'un fournisseur - et observe les échanges depuis plusieurs semaines. Il connaît le numéro de la prochaine facture, le nom de l'interlocuteur habituel et les dates de congés. L'IA ne sert qu'à imiter le ton, la voix ou le visage.

### Quels sont les scénarios les plus fréquents ?

| Scénario | Présentation | Signal à repérer |
|---|---|---|
| **Le faux fournisseur** | Un courriel annonce de nouvelles coordonnées bancaires, avant une facture attendue | Toute modification de RIB, quelle que soit la crédibilité du message |
| **Le faux dirigeant** | Un appel, un message vocal ou une visioconférence demandent un virement urgent pour une opération confidentielle | La demande de secret et le contournement de la procédure habituelle |
| **Le faux conseiller bancaire** | Un appel propose de « sécuriser » un compte en faisant valider une opération | Une banque ne demande jamais de valider une opération qu'elle vient de signaler |
| **Le faux support informatique** | Un technicien demande l'installation d'un logiciel de prise en main à distance | Toute demande d'accès à distance non sollicitée |

### Ce qui change

| Le réflexe de vérification d'hier | Pourquoi il ne suffit plus |
|---|---|
| **Repérer les fautes dans un courriel** | Le texte est correct et reprend le style habituel de l'expéditeur |
| **Reconnaître la voix au téléphone** | La voix est clonée à partir d'un extrait public, intonations comprises |
| **Rappeler pour confirmer** | Le numéro affiché peut être usurpé, et l'interlocuteur être un clone |
| **Demander une visioconférence** | Le visage et la voix se truquent également en direct |

© ATH. Tous droits réservés.

Un filet de sécurité est apparu du côté des banques : depuis octobre 2025, celles-ci vérifient la cohérence entre le nom du bénéficiaire et l'IBAN avant l'exécution d'un virement. Ce contrôle est utile mais insuffisant, un fraudeur pouvant ouvrir un compte au nom exact du fournisseur usurpé.

## Concrètement pour l'entreprise

### *Prévenir*

- **Formaliser une règle non négociable sur les virements.** Au-delà d'un seuil défini par l'entreprise, deux personnes valident et la vérification emprunte un canal différent de celui de la demande.
- **Traiter tout changement de RIB comme suspect**. Rappel du fournisseur au numéro figurant sur le contrat, jamais celui du message, et confirmation écrite avant tout paiement.
- **Convenir d'un mot de passe interne** entre le dirigeant et les personnes habilitées à payer, jamais consigné dans un courriel.
- **Sécuriser les messageries.** Double authentification sur l'ensemble des boîtes, en priorité celles de la direction et de la comptabilité : l'intrusion initiale s'y produit le plus souvent.
- **Mesurer l'exposition publique.** Organigramme détaillé en ligne, absences du dirigeant annoncées sur les réseaux, vidéos où il s'exprime longuement : autant de matière exploitable. Il ne s'agit pas de disparaître, mais de choisir ce qui est diffusé.

### *Organiser*

- **Retirer à l'urgence son pouvoir.** Indiquer aux équipes qu'aucun reproche ne sera formulé pour un paiement différé le temps d'une vérification. La mesure est la plus efficace et n'a aucun coût.
- **Former l'ensemble des personnes pouvant déclencher un paiement** ou transmettre un document, et pas la seule comptabilité : trente minutes par an sur des cas réels suffisent à installer le réflexe.
- **Vérifier les garanties d'assurance.** Les couvertures visant ce type de fraude supposent fréquemment une procédure écrite et des équipes formées, à défaut de quoi elles ne s'appliquent pas.

### *Que faire si un virement frauduleux est parti ?*

- Contacter immédiatement la banque et demander le rappel des fonds : les chances de récupération diminuent d'heure en heure.
- Conserver l'intégralité des preuves - courriels complets, numéros, messages vocaux - sans suppression ni transfert.
- Déposer plainte et solliciter l'assistance de cybermalveillance.gouv.fr.
- Déclarer le sinistre à l'assureur dans le délai prévu au contrat, souvent très court.
- Informer le fournisseur ou l'interlocuteur usurpé, dont la messagerie est peut-être compromise et d'autres clients exposés.

## Les points de vigilance

- Chercher à démasquer l'imitation à l'oreille est sans issue. Ce qui se détecte, c'est le scénario : urgence, confidentialité demandée, canal inhabituel.
- Une procédure contournée par le dirigeant lui-même en cas d'urgence ne tient pas trois mois.
- Les attaques visent les moments de moindre vigilance : vendredi soir, veille de congés, période de clôture, absence du dirigeant.
- Un premier virement de faible montant sert parfois à tester la vigilance de l'entreprise avant une demande plus importante.

## À savoir

Parmi les mesures énumérées, deux suffisent à bloquer la grande majorité des tentatives : la double validation sur un canal indépendant, et le rappel au numéro figurant au contrat. Les autres viennent ensuite, par ordre d'exposition.

Une procédure jamais éprouvée reste théorique. Un test sans annonce préalable, une fois par an, constitue le seul moyen de vérifier qu'elle est réellement appliquée.

## À retenir

1. La voix, le visage et le numéro affiché ne constituent plus des preuves d'identité.
2. Une règle écrite de double validation, sur un canal indépendant, neutralise même une imitation parfaite.
3. Tout changement de coordonnées bancaires se vérifie par un rappel au numéro déjà détenu par l'entreprise.
4. La messagerie est souvent la porte d'entrée : double authentification sur les boîtes sensibles.
5. En cas de virement frauduleux, les premières heures déterminent les chances de récupération des fonds.

### *Pour aller plus loin*

Cybermalveillance.gouv.fr - fiche réflexe « *fraude au virement bancaire* » et rapport d'activité 2025.

Règlement (UE) 2024/886 - vérification du bénéficiaire par les banques avant virement.

© ATH. Tous droits réservés.