CERCLE IA · FICHE-MÉMO

Incident ou arnaque liés à l'IA : vers qui se tourner, dans quel ordre

Ce qui arrive.
Un virement part vers un faux compte, une messagerie est piratée, des fiches clients finissent dans un compte d'IA personnel, un assistant envoie ce qu'il ne devait pas.

Ce qui coûte cher.
Appeler dans le désordre, ou sans preuves : la banque attend la plainte, les enquêteurs attendent les messages, le prestataire attend les dates.

Ce que contient la fiche.
Un arbre en cinq situations, le premier interlocuteur de chacune, ce qu'on lui apporte, puis huit questions pour être prêt.

Pour les dirigeants de TPE et les indépendants, partout en France, qui viennent de vivre un incident ou une arnaque liés à l'IA

Édition du 19/11/2026 · NLQ

01 Nommez d'abord ce qui s'est passé

Il n'existe pas de guichet « incident IA ». L'IA change la forme de l'arnaque ou de l'erreur, pas la porte à pousser. Le dispositif national Cybermalveillance.gouv.fr assiste les victimes, entreprises comprises, et propose un diagnostic en ligne, gratuit, sans information personnelle demandée.

1 **Argent parti ?** Banque → 2 **Compte pris ?** Service du compte → 3 **Données sorties ?** Fiche d'incident, CNIL → 4 **Assistant de travers ?** Couper, prestataire → 5 **Rien de clair ?** Diagnostic en ligne

CE QUI S'EST PASSÉ	PREMIER INTERLOCUTEUR	CE QU'ON APPORTE
Virement vers un faux RIB ou sur une demande urgente	Votre banque, tout de suite	Ordre de virement, messages reçus, facture
Messagerie ou compte d'un outil IA piraté	Le service qui gère le compte	Captures des connexions et réglages suspects
Données de clients ou de salariés collées dans un outil grand public	La personne qui tient vos données, puis la CNIL	Ce qui est parti, combien, depuis quel compte
Assistant qui a envoyé, modifié ou supprimé	Celui qui a branché l'assistant, puis un prestataire labellisé	Journal, heure, ce qui a changé
Vous ne savez pas	Le diagnostic en ligne de Cybermalveillance.gouv.fr	Le récit des faits, dans l'ordre

Plusieurs branches à la fois ? Commencez par l'argent, puis le compte : c'est souvent un compte pris qui a permis le faux virement.

02 Argent parti : la banque d'abord, la plainte ensuite

Cybermalveillance.gouv.fr décrit l'escroquerie aux faux ordres de virement comme un virement non planifié obtenu par persuasion, menaces ou pressions, souvent présenté comme « urgent et confidentiel ». Une voix au téléphone ou une vidéo qui ressemble à votre dirigeant ou à un fournisseur ne change rien à la marche à suivre. Pour un cas de faux RIB raconté pas à pas, voir notre étude de cas sur cercle-ia.com.

Alertez votre banque immédiatement.
Elle peut tenter de suspendre le virement s'il n'est pas encore effectué ; sinon, demandez le retour des fonds. Elle pourra exiger une copie du dépôt de plainte.

Listez tous les virements concernés.
Ceux exécutés, en instance ou à venir vers les coordonnées frauduleuses, et faites bloquer ces coordonnées dans vos logiciels (fiche FOVI).

Prévenez le créancier dont on a pris l'identité.
Sa messagerie a peut-être été piratée.

Déposez plainte dans les plus brefs délais.
Au commissariat, à la brigade de gendarmerie, ou par écrit au procureur de la République, avec toutes les preuves en votre possession.

03 Compte pris : reprenez la main, puis prévenez

Un compte de messagerie piraté sert souvent de point de départ au faux RIB, selon Cybermalveillance.gouv.fr. Un compte d'outil IA se protège de la même façon : mot de passe propre à ce service, double authentification. Le pirate laisse parfois des portes ouvertes pour revenir.

Contactez le service concerné.
Si vous ne pouvez plus vous connecter, signalez le piratage et demandez la réinitialisation du mot de passe.

Fermez les portes laissées.
Adresse et numéro de récupération inconnus, redirections, règles de filtrage, sessions actives qui ne sont pas les vôtres : capture d'écran d'abord, suppression ensuite.

Changez le mot de passe partout où il servait.
Puis activez la double authentification si le service la propose.

Prévenez vos contacts et vérifiez les commandes.
Qu'ils ne soient pas escroqués en votre nom ; prévenez la banque si des coordonnées bancaires étaient dans le compte.

04 Données parties dans un outil grand public : documentez, puis voyez la CNIL

Cybermalveillance.gouv.fr cite les partages non maîtrisés de données parmi les risques de l'IA, et conseille aux salariés d'utiliser exclusivement le service souscrit par l'employeur. Quand des données de clients sont déjà parties, la CNIL décrit ce qu'elle attend d'un responsable de traitement.

Écrivez la fiche d'incident.
Dans tous les cas, selon la CNIL : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements, conséquences probables, mesures prises.

Limitez la suite.
Paramètres de confidentialité du compte, historique effacé si le service le permet, et rappel de la règle : pas de compte personnel pour le travail.

Notifiez si la CNIL le demande.
En cas de risque pour les personnes, dans les meilleurs délais, avec une notification initiale dans un délai de 72 heures si possible ; en cas de doute, la CNIL demande qu'on lui notifie.

Ne tranchez pas seul.
Savoir si votre cas est une violation ne se décide pas dans cette fiche : lisez la page de la CNIL.

05 Assistant qui a agi de travers : arrêtez-le, gardez la trace

Un assistant branché à votre messagerie ou à vos fichiers peut envoyer, modifier ou supprimer. Cybermalveillance.gouv.fr conseille de limiter au strict nécessaire ses autorisations, dont les actions automatiques sans confirmation humaine. Quand l'erreur est faite, l'ordre compte.

Coupez ses droits d'écriture.
Retirez l'autorisation d'envoyer ou de modifier ; laissez la lecture si elle sert à comprendre.

Revenez à la façon de faire sans IA.
L'ANSSI recommande de prévoir un mode dégradé des services métier sans système d'IA (R15) : la personne qui faisait le travail avant reprend la main.

Gardez le journal.
Les demandes, les outils appelés, les réponses : l'ANSSI recommande de journaliser l'ensemble des traitements (R29).

Faites-vous assister.
Les prestataires labellisés ExpertCyber, après un audit réalisé par l'AFNOR, couvrent l'assistance en cas d'incident ; la plateforme permet de vérifier un label. Si l'erreur vient d'un compte piraté, passez à la branche précédente.

06 Préparez ce qu'on vous demandera

La banque, les enquêteurs et le prestataire posent les mêmes questions : quoi, quand, par où. Cybermalveillance.gouv.fr rappelle que ces éléments peuvent servir de preuves en cas de procédure.

Une chronologie.
Heure de chaque message, appel, virement, connexion suspecte, et ce que vous avez déjà fait.

Les preuves telles quelles.
Messages et mails reçus, numéros qui vous ont appelé, ordres de virement, factures, relevés, captures d'écran des réglages modifiés.

La liste des comptes touchés.
Messagerie, banque, outils d'IA, avec la personne qui les gère.

Le récépissé de plainte.
Service-Public.fr rappelle de le conserver : c'est la preuve du dépôt, et la banque peut la demander.

Comment savoir si c'est en place

Huit questions fermées. Chaque « non » renvoie à une branche.

- [ ] Savez-vous qui appeler à votre banque pour un virement frauduleux ?
- [ ] La double authentification est-elle active sur la messagerie et les comptes d'outils d'IA ?
- [ ] Savez-vous retirer à votre assistant le droit d'envoyer ou de modifier ?
- [ ] Gardez-vous la trace de ce que fait l'assistant ?
- [ ] Une demande de virement imprévue passe-t-elle par une validation interne qu'on ne contourne pas ?
- [ ] Chaque salarié utilise-t-il le service d'IA de l'entreprise, et non un compte personnel ?
- [ ] Le travail confié à l'assistant peut-il reprendre sans lui ?
- [ ] Savez-vous où trouver un prestataire labellisé avant d'en avoir besoin ?

VOTRE PROCHAINE ÉTAPE

Une fois l'urgence passée, venez avec ce qui s'est produit : on regarde ensemble quelle porte vous avez poussée, et ce qu'il faut préparer pour la prochaine fois.

Réserver un échange gratuit

www.cercle-ia.fr/rendez-vous/

Sources et portée

Toutes les sources ont été ouvertes le 19/11/2026.

- Cybermalveillance.gouv.fr, *Qu'est-ce que le GIP ACYMA ?* https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous (consulté le 19/11/2026)
- Cybermalveillance.gouv.fr, *Diagnostic*. https://www.cybermalveillance.gouv.fr/diagnostic/accueil (consulté le 19/11/2026)
- Cybermalveillance.gouv.fr, *Prestataires référencés et labellisés*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/page/prestataires (consulté le 19/11/2026)
- Cybermalveillance.gouv.fr, fiches réflexes *Fraude au virement ou faux RIB*, *Faux ordres de virement (FOVI)*, *Piratage de compte*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fraude-au-virement-ou-au-faux-rib ; https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/escroquerie-faux-ordres-virement-fovi ; https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-de-compte (consultés le 19/11/2026)
- Cybermalveillance.gouv.fr, *Utiliser l'IA : conseils pour les particuliers et les professionnels*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/utiliser-ia-conseils-pour-les-particuliers-et-les-professionnels (consulté le 19/11/2026)
- Cybermalveillance.gouv.fr, *Déposer plainte suite à une cybermalveillance*. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/page/deposer-plainte-cybermalveillance (consulté le 19/11/2026)
- CNIL, *Notifier une violation de données personnelles*. https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles (consulté le 19/11/2026)
- ANSSI, guide ANSSI-PA-102 *Recommandations de sécurité pour un système d'IA générative*, version du 29/04/2024 : R15, R29. https://messervices.cyber.gouv.fr/documents-guides/Recommandations_de_s%C3%A9curit%C3%A9_pour_un_syst%C3%A8me_d_IA_g%C3%A9n%C3%A9rative.pdf (consulté le 19/11/2026)
- Service-Public.fr, *Porter plainte*. https://www.service-public.gouv.fr/particuliers/vosdroits/F1435 (consulté le 19/11/2026)

Portée : l'ordre des branches est proposé par cette fiche ; les exemples sont fictifs. Aucun numéro d'appel n'est donné : prenez-les sur la fiche officielle de votre branche. Ni avis juridique, ni garantie de récupérer des fonds.

Édité par NLQ — Cercle IA (www.cercle-ia.fr), avec le soutien d'ALMA, sponsor. Édition du 19/11/2026. Exemples fictifs ; ce qui est dit des textes cités vient des sources datées ci-dessus.