Nexia S&A

Guide de la fraude à l'ère de la facturation électronique

Avant-propos

La réforme de la facture électronique, dont le déploiement obligatoire débute au 1er septembre 2026, représente une transformation majeure des flux financiers des entreprises françaises. Elle crée de nouvelles opportunités opérationnelles, mais elle ouvre aussi une **fenêtre d'exposition inédite** aux fraudeurs.

En parallèle, les experts en cybersécurité constatent une double dynamique : les attaques sont à la fois plus **nombreuses** (massification) et plus **sophistiquées** (ciblage chirurgical).

L'intelligence artificielle abaisse la barrière d'entrée pour les cybercriminels, qui s'organisent désormais comme de véritables entreprises avec des équipes spécialisées, un service après-vente et des plans de continuité d'activité.

Face à cette réalité, la question n'est plus « *serons-nous attaqués* ? » mais « *sommes-nous prêts à y faire face* ? »

La facture électronique est une double opportunité : si elle est une obligation c'est aussi un moyen d'améliorer le contrôle des transactions, d'offrir une piste d'audit fiable et de réduire drastiquement la fraude.

Ce guide a été conçu pour vous informer et vous sensibiliser sur les risques auxquels vous êtes et/ou serez de plus en plus exposés. La grande majorité des fraudes réussies exploitent des failles connues et évitables : un contrôle insuffisant sur les coordonnées bancaires, un mot de passe enregistré dans un navigateur, une urgence fabriquée qui court-circuite le bon sens.

SOMMAIRE

À jour au 1er mars 2026

© - ATH tous droits réservés

1 Pourquoi les fraudes explosent maintenant ?

a. Une dynamique confirmée : plus de flux numérisés, plus de surface d'attaque

59 %
des PME participantes ont subi une cyber-attaque au cours des 12 derniers mois [1].

33 %
ont dû verser une rançon importante après un cyber-incident.

+26 %
de tentatives de phishing bloquées dans le monde en 2024 par Kaspersky, vs 2023.

125 millions
d'attaques impliquant des pièces jointes malveillantes détectées en 2024.

1 sur 2
emails professionnels est un spam.

En france en 2024

23 millions
de tentatives de phishing bloquées.

500 000
pièces jointes malveillantes bloquées.

Des outils d'attaques accessibles à des profils sans compétence technique grâce à l'intelligence artificielle. Les groupes criminels utilisent des méthodes de plus en plus sophistiquées comme de vraies entreprises, avec des équipes dédiées à la reconnaissance, à l'attaque, au service client (oui, ils en ont un), et à la revente d'accès compromis.

Le phénomène de massification et de sophistication ne s'oppose pas, mais ils se combinent : les campagnes massives servent à repérer les cibles vulnérables, les accès obtenus sont ensuite revendus à des groupes plus sophistiqués pour des attaques ciblées.

Ce que cela signifie pour votre entreprise : vous n'êtes pas trop petit pour être ciblé. Vous êtes une cible parce que vous avez une trésorerie, des fournisseurs, des clients et des données.

b. L'IA change les règles du jeu

L'intelligence artificielle générative a supprimé les indicateurs traditionnels de la fraude :

Avant

Un mail phishing se reconnaissait à ses fautes d'orthographe, son style maladroit, ses formulations approximatives.

Aujourd'hui

Les messages frauduleux sont parfaitement rédigés, personnalisés, adaptés à l'actualité de l'entreprise (levée de fonds récente, contexte de la réforme fiscale, actualité sectorielle). Même des experts reconnaissent avoir failli se laisser piéger.

[1] D'après le rapport 2025 d'HISCOX sur la gestion des risques cyber.

© - ATH tous droits réservés

La réforme impose des flux via les plateformes agréées et un annuaire/concentrateur, ce qui transforme profondément la chaine de transmission traditionnelle jusqu'alors « *facture* → *comptabilité* → *paiement* → *TVA* ».

c. Les criminels travaillent comme des entreprises : organisation, spécialisation, ciblage

Les groupes de criminels d'aujourd'hui ressemblent davantage à des start-ups qu'à des hackers isolés, par exemple Storm 0539 [2] et leur attaque sur l'entreprise émettrice de cartes cadeaux.

Spécialisation des tâches :

Collecteurs d'accès, développeurs de malwares, opérateurs, communicants, négociateurs.

Horaires de bureau :

Certains fonctionnent de 09h à 18h, avec des niveaux de disponibilité et réactivité supérieurs à beaucoup d'équipes IT légitimes.

Service après-vente :

Vente d'identifiants avec garantie de remboursement si invalides, support multi-langues.

Plan de continuité :

Une infrastructure démantelée est reconstruite en quelques jours.

Ce n'est plus un problème informatique, c'est un problème de gestion des risques de l'entreprise, au même titre que le risque client ou le risque fournisseur.

d. La frontière pro/perso : le vrai angle mort des dispositifs de contrôle

Depuis le covid, les modes de travail ont profondément évolué. La séparation entre usage professionnel et personnel s'est érodée progressivement :

- Un ordinateur portable professionnel peut être utilisé aussi pour des achats personnels,
- Les mots de passes professionnels enregistrés dans le navigateur à côté des mots de passe personnels,
- Les comptes de messagerie professionnelle connectés à des services tiers non sécurisés,
- Les applications personnelles (WhatsApp, Google, cloud perso) utilisées pour des échanges professionnels,

Ces comportements créent des vecteurs d'attaques invisibles. L'attaquant compromet d'abord l'environnement personnel, puis pivote vers le professionnel.

---

[2] *Cyber Signals : Comprendre le risque croissant de fraude aux cartes-cadeaux, par Vasu, vice-président de Microsoft Security.*

© - ATH tous droits réservés

2 Comprendre la réforme et ses effets sur la fraude

a. Ce que la réforme numérise réellement

Pendant des décennies, vous avez traité des factures. Demain, vous traiterez la donnée, et c'est celle-là qui travaillera pour vous.

La réforme ne concerne pas la technologie. Elle redéfinit trois fondamentaux :

Le flux, pas le document

Avant	Aujourd'hui
Une facture arrive (papier, email, PDF...). Vous la lisez, la saisissez, la classez.	Une facture se transmet. Elle se lit elle-même, se valide (via un contrôle), et même s'archive automatiquement.

L'intelligence, pas la main d'œuvre

Avant	Aujourd'hui
Vos collaborateurs extraient, contrôlent, enregistrent. Travail répétitif, source d'erreurs.	Les systèmes échangent des données intelligentes. Les humains pilotent, analysent, décident.

Le dialogue continu, pas l'échange isolé

Avant	Aujourd'hui
Une facture = une transaction fermée. Le fournisseur envoie, le client reçoit. Point final.	Le fournisseur et le client dialoguent en temps réel à travers leur plateforme agréée. Correction, validation, paiement : tout s'orchestre numériquement.

La facture n'est plus un objet à traiter. C'est une donnée vivante qui s'échange, se valide, s'exploite sans intervention manuelle.

La comptabilité n'est plus une tâche fastidieuse. Elle évolue vers un système automatisé et maîtrisé.

La traçabilité n'est plus une confiance déclarative. C'est une preuve numérique incontestable.

La réforme numérise la chaine de valeur comptable elle-même.

Pas vos outils. Pas votre paperasse, mais votre métier.

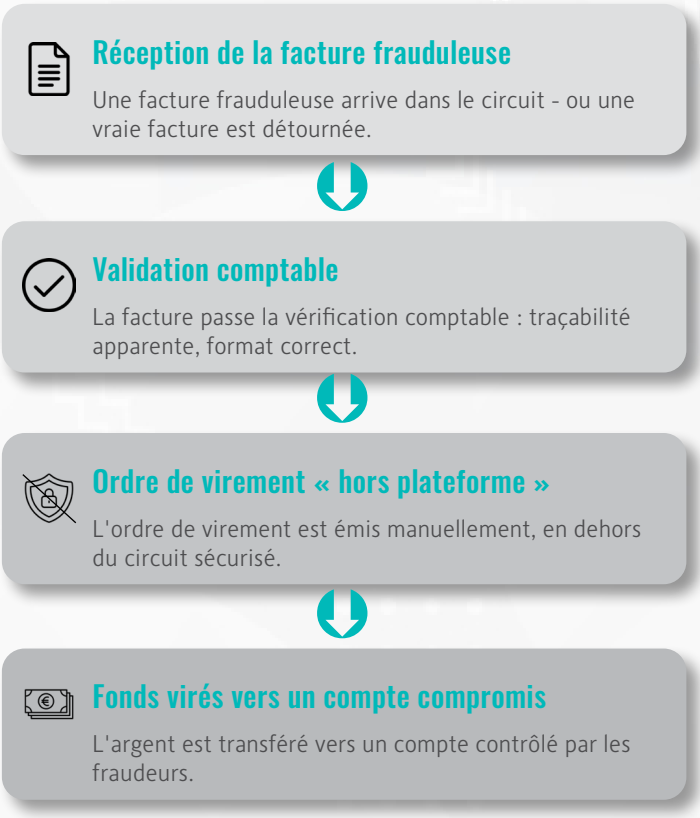
© - ATH tous droits réservés

b. Principe directeur : « plus de traçabilité ≠ moins de fraude » si le paiement reste contournable

Acte 1 : la faille identifiée

La facture est numérisée. Vous la tracez parfaitement. Mais le paiement ? Il sort du système.

Schéma de la fraude



Le paradoxe : Vous avez tracé 100 % de la facture. Vous avez en sécurisé 0 % du paiement.

La réforme a fermé une porte, le fraudeur passe par la fenêtre.

© - ATH tous droits réservés

Acte 2 : La réduction du risque

Avec les solutions de paiement intégré, le flux devient complet et blindé :

- Facture numérisée (traçabilité complète),
- Paiement au sein de la plateforme agréée (authentification, cryptage...),
- Validation double : données facture + instruction paiement,

Le gain : le fraudeur n'a plus d'espace de manœuvre. Il ne peut pas émettre un virement parallèle ; tout transite par un système sécurisé et audité.

Réduction drastique des fraudes « *facture + redirection bancaire* ».

Acte 3 : le vrai enjeu

Mais voilà le problème :

Un système techniquement sécurisé peut être contourné par l'humain.

Trois risques demeurent :

L'humain autorise la fraude

- Collaborateur compromis qui valide une fausse facture, même dans une PA,
- Manager qui ignore les procédures.

La fraude monte en amont

- Factures en dehors du circuit sensible (meubles, petits services),
- Factures de prestataires non standardisés.

Le compte fournisseur lui-même est compromis

- Pas de fraude « facture » : le compte du vrai fournisseur est piraté,
- Les paiements légitimes vont à des pirates.

© - ATH tous droits réservés

c. La complexité réglementaire comme terrain de chasse

La réforme de la facturation électronique ne repose pas sur un acteur unique, mais sur un écosystème multi-niveaux que peu d'entreprises maîtrisent réellement. Cette architecture comprend trois acteurs distincts, chacune avec des prérogatives spécifiques.

Pour rappel :

Le Portail public de facturation **(PPF)**, déployé par l'AIFE, est la colonne vertébrale administrative du dispositif. Il remplit deux missions clés : **gérer l'annuaire central** d'identification des émetteurs/destinataires, et **collecter les données** de facturation, transaction et paiement pour le compte du fisc.

Les Plateformes Agréées (PA) sont des opérateurs privés immatriculés par l'État, chargés de **l'opérationnel du dispositif** : échange, contrôle et transmission des factures électroniques, tout en garantissant leur authenticité et l'interopérabilité entre acteurs. Elles assurent aussi la remontée des données e-invoicing/e-reporting vers l'administration fiscale. En option, elles peuvent proposer des services à valeur ajoutée : **archivage probant** et **paiement automatisé** des factures.

Et **les Solutions Compatibles (SC)** accompagnent les entreprises en amont/aval des PA (construction de factures, rapprochement, paiement), mais sans immatriculation : elles ne transmettent ni ne reçoivent de factures.

Cette architecture à trois niveaux créée une confusion exploitable : qui est légitime ? Qui fait quoi ? Ou vérifier ?

Chaque obligation génère un prétexte

Un email arrive : « *Votre entreprise doit valider son immatriculation au Portail Public de Facturation avant le [date]. Cliquez ici pour mettre à jour vos informations.* »

Le fraudeur détourne la réalité du PPF (qui existe effectivement) pour créer une urgence fictive. La victime, qui sait vaguement qu'un « *portail public* » existe, ne fait pas la différence entre :

- Une vraie obligation (transmettre ses factures via une PA),
- Une fausse injonction (s'immatriculer manuellement sur un faux portail).

Le lien redirige vers une interface clone où l'entreprise saisit ses identifiants de plateforme, son SIRET, voire son RIB pour de prétendus « *frais administratifs* ».

Plus l'écosystème est complexe, plus il est difficile de distinguer le légitime du frauduleux. Le fraudeur ne crée par la complexité, il l'exploite. Chaque technique de distinction (PA, solution compatible, annuaire, concentrateur) devient un angle d'attaque.

L'ignorance légitime se transforme en vulnérabilité opérationnelle.

© - ATH tous droits réservés

Quelques gestes à adopter

Vérifier l'annuaire officiel	Avant toute action, consulter l'annuaire du PPF (site officiel uniquement, jamais via un lien email) pour vérifier l'existence d'un acteur.
Ne jamais cliquer sur un lien de mise en conformité	Passer par votre PA habituel ou le site officiel du PPF (URL tapée manuellement).
Former les équipes	30 minutes suffisent pour expliquer qui fait quoi (PA, SC, PPF) et comment vérifier la légitimité d'une demande.

La complexité devient une vulnérabilité uniquement si elle reste opaque. Clarifier les rôles et adopter une défiance méthodique neutralise ce risque.

La double sanction : une fraude peut être simultanément pénale et fiscale

La fraude à la facturation ne se limite pas aux pertes financières potentielles qu'elle engendre. Elle expose les entreprises à des sanctions fiscales souvent plus sévères que le préjudice initial.

L'administration peut refuser la déduction de la charge et la récupération de la TVA dès lors qu'elle n'est pas en mesure de vérifier la réalité économique de l'opération, quel que soit le degré de bonne foi de l'entreprise.

© - ATH tous droits réservés

3 Cartographie des fraudes à connaître

a. Les fraudes au paiement, impact immédiat sur la trésorerie

Les menaces les plus courantes auxquelles les entreprises sont confrontées :

La fraude au président

Un fraudeur usurpe l'identité d'un dirigeant de l'entreprise (par mail ou appel) pour exiger un virement urgent et confidentiel.

L'arnaque au faux fournisseur (ou fraude au RIB)

Cette technique de manipulation, consiste pour un malfaiteur à usurper l'identité d'un partenaire commercial légitime.

L'objectif principal est d'inciter la victime à modifier les coordonnées bancaires de règlement pour détourner les fonds. En usurpant ces informations, les fraudeurs parviennent à intercepter des **virements financiers** importants avant que la supercherie ne soit découverte.

Détournement de virement par compromission de messagerie (BEC)

Le *Business Email Compromise*, est un type de cyberattaque dont l'objectif est de prendre le contrôle d'une messagerie professionnelle pour l'utiliser à des fins malveillantes. Concrètement, cette fraude repose sur la **manipulation malveillante des conversations par e-mail** pour tromper une victime.

La fraude à la TVA

Création de factures fictives pour obtenir des remboursements de TVA indus, ou altération des montants de la TVA pour réduire la charge fiscale.

La fraude interne

Des employés créent des fausses factures ou gonflent les prix des fournisseurs légitimes. C'est une fraude complexe à détecter car elle implique une manipulation des systèmes de l'intérieur.

© - ATH tous droits réservés

b. Les fraudes documentaires et d'identité

- **Fraude à l'annuaire :** modification d'adresse de facturation, détournement de routage,
- **La fraude à la fausse facture :** des escrocs ou des fournisseurs fantômes envoient des factures pour des biens ou des services qui n'ont pas été livrés ou réalisés.
- **L'usurpation d'identité du fournisseur.**

c. Les fraudes cyber qui ouvrent la voie aux fraudes financières

Les Cyberattaques :

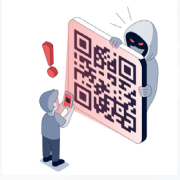
Interception de factures lors de leur envoi pour modifier les données de paiement, ou piratage direct des plateformes de facturation électronique, ou des postes d'utilisateur client pour voler des informations bancaires et des numéros de TVA.

Le Phishing (hameçonnage) :

C'est une technique frauduleuse qui consiste à usurper l'identité d'un tiers de confiance, principalement par courriel, dans le but de tromper la victime et de lui soutirer des données personnelles, des mots de passe ou des coordonnées bancaires.

Le Smishing :

C'est une contraction de SMS et de Phishing, il s'agit d'une variante de l'hameçonnage diffusée par SMS ou via des applications de messagerie sur téléphone mobile. Le message incite la victime à agir dans l'urgence en cliquant sur un lien piégé ou en rappelant un numéro frauduleux.



Le Quishing :

C'est une contraction de QR code et de Phishing, cette attaque utilise des codes QR malveillants. Une fois scannée avec un smartphone, le faux QR code redirige la victime vers un site frauduleux conçu pour voler ses informations sensibles ou pour télécharger un logiciel malveillant sur son appareil.

Le Compromission de comptes de service (BEC - Business email Compromise) :

Mécanisme :

L'attaquant prend le contrôle de la boîte e-mail d'un dirigeant, d'un DAF ou d'un responsable achat. Il lit les échanges pendant des semaines, comprend les procédures, identifie les projets en cours, puis intervient au moment opportun pour modifier les instructions de paiement.

Caractéristique dangereuse :

L'entreprise ne sait pas que sa messagerie est compromise. Les e-mails semblent authentiques car ils le sont.

Signal d'alerte :

Règle de transfert automatique créée discrètement, connexion depuis un pays inhabituel, connexion à des horaires anormaux.

© - ATH tous droits réservés

Vol de session navigateur :

Mécanisme :

L'attaquant vole le cookie de session du navigateur (qui prouve que vous sous êtes authentifié). Il peut alors se connecter à vos comptes sans avoir besoin de votre mot de passe ni de votre double authentification (MFA).

Vecteurs :

Extensions de navigateur malveillantes, sites web piégés, synchronisation perso/pro.

Compromission d'un prestataire (attaque par la chaine d'approvisionnement) :

Mécanisme :

L'attaquant cible un fournisseur IT (éditeur logiciel, PA, SC, cabinet d'expertise comptable...) pour accéder ensuite à ses clients. Un accès légitime, via un compte de service ou un *token API*, ne déclenche aucune alerte.

Exemples réels :

SolarWinds (2020), compromissions de CRM (SalesForce, HubSpot), attaques via des paquets npm/PyPI.

Courtier en accès initial (Initial Access Brokers) :

Mécanisme :

Des logiciels malveillants (« *stealers* ») collectent automatiquement tous les identifiants enregistrés dans le navigateur, les cookies de session, les mots de passe enregistrés. Ces données sont revendues sur des marchés du dark web.

« *Ils vendent au kilomètre des accès. C'est du pick and choose : choisis là-dedans les victimes qui t'intéressent* ». Expert cybersécurité, Risk Intel Media 2025.

© - ATH tous droits réservés

4 Les signaux d'alerte (red flags)

Il est crucial d'apprendre aux collaborateurs à repérer les éléments suspects. Voici quelques-uns qui doivent éveiller les soupçons :

- **L'urgence et le secret :** c'est le levier psychologique principal des fraudeurs. Toute demande de paiement « *immédiat* » assortie d'une consigne de confidentialité doit alerter.
- **Anomalie sur les factures :** des montants anormalement élevés, des fractions de centimes inhabituelles, ou encore l'absence d'informations obligatoires comme le numéro de TVA intracommunautaire.
- **Détails visuels trompeurs :** Une adresse e-mail presque identique à celle du fournisseur habituel, à une lettre près (ex : info@gestion-strategie.fr au lieu de info@gestion-strategies.fr).
- **Incohérence des données :** une adresse de facturation différente de l'adresse habituelle, un fournisseur inconnu, ou la réception de la même facture en double.

5 Scénarios typiques à anticiper avec la réforme

Scénario 1 - « Activation / Migration Plateforme Agréée »

La situation

Vous recevez un e-mail (ou un SMS, ou un appel) vous demandant de :

- Finaliser votre action sur la Plateforme Agréée,
- Mettre à jour vos paramètres de réception,
- Valider un test de connexion pour le e-invoicing,
- Confirmer votre mandat pour la transmission de données à l'administration fiscale via le e-reporting.

Ce qui se passe réellement

Vous êtes redirigé vers un faux portail qui ressemble à votre vraie PA.

Vous renseignez vos identifiants et mot de passe → le fraudeur les récupère.

Il se connecte à votre vrai compte, modifie les paramètres (RIB, e-mail de contact), crée un accès permanent.

La règle d'or

Toute action sur votre PA doit être initiée par **vous**, depuis un lien enregistré dans vos favoris ou votre saisie dans la barre https, mais **jamais** depuis un lien reçu par e-mail.

© - ATH tous droits réservés

Scénario 2 - « Faux support technique / Faux intégrateur »

La situation

Vous recevez un appel d'une personne se présentant comme le support de votre solution compatible ou de votre Plateforme Agréée. Elle vous explique que votre paramétrage est incomplet, qu'il y a une anomalie, qu'il faut intervenir en urgence.

Elle vous demande de :

- Installer un outil d'accès à distance (*TeamViewer, AnyDesk*),
- Valider une notification MFA (*Multi Factor Authentification*),
- Partager votre écran.

Ce qui se passe réellement

Des attaquants ou groupe similaires qui excellent dans l'ingénierie sociale, qui jouent sur l'autorité technique et l'urgence.

Une fois le contrôle obtenu, ils créent des accès persistants et préparent une fraude financière.

La règle d'or

Aucun vrai support ne vous demandera jamais de valider un MFA par téléphone, ni d'installer un outil d'accès à distance sans procédure formelle préalable.

Scénario 3 - « Changement de RIB dans la vague de mise à jour fournisseurs »

La situation

Dans les semaines précédant le 1er septembre 2026, voire après, votre équipe comptable reçoit de nombreuses demandes de mise à jour de la part de fournisseurs qui « *se conforment à la réforme facturation électronique* » et doivent « *mettre à jour leurs coordonnées* ».

Au milieu de ces demandes légitimes, une demande frauduleuse passe sous les radars : même ton, même contexte, nouveau RIB « *pour la facturation électronique* ».

Ce qui se passe réellement

C'est une fraude classique au changement de RIB, rendue invisible par le contexte de la réforme.

La règle d'or

Le contexte de la réforme ne change rien à la procédure de changement de RIB. Chaque demande de modification bancaire suit le protocole complet, sans exception ni raccourci.

© - ATH tous droits réservés

Scénario 4 - « Compromission du compte de service / API PA »

La situation

Votre intégrateur vous remet des clés API pour connecter votre ERP à votre PA.

Ces clés sont stockées dans un fichier de configuration, un e-mail archivé, ou un outil de gestion de projet.

Ce qui se passe réellement

Un attaquant qui compromet l'environnement du prestataire, ou scanne vos fichiers, trouve ces clés. Il s'en sert pour :

- Exfiltrer toutes vos données de facturation (clients, montants, fréquences),
- Modifier des paramètres de routage (où partent vos factures),
- Préparer une fraude à grande échelle.

La règle d'or

Les secrets (clés API, *tokens*) ne se partagent jamais par e-mail. Ils sont stockés dans un coffre-fort dédié, avec droits minimaux et rotation planifiée.

Scénario 5 - « Mail de phishing contextuel post-levée de fonds / Regroupement / Actualité »

La situation

Votre entreprise vient de réaliser une opération visible (levée de fonds, acquisition, appel d'offres, article de presse).

Dans les jours suivants, vos collaborateurs reçoivent des e-mails parfaitement rédigés, avec le bon logo, le bon contexte : « *votre augmentation suite à la croissance de l'entreprise* », « *mise à jour RH post-acquisition* », « *accès au nouveau portail fournisseur* ».

Ce qui se passe réellement

Les attaquants surveillent l'actualité économique en temps réel, utilisent l'IA pour générer des messages personnalisés et déclenchent leurs campagnes dans les 24-48h suivant un événement.

La règle d'or

Tout document, lien ou instruction qui arrive par e-mail et concerne une action financière ou d'accès doit être validé hors e-mail, même si le contenu semble parfaitement légitime.

© - ATH tous droits réservés

6 Les bonnes pratiques et mesures préventives

a. Les contrôles à réaliser qui stoppent 80 % des fraudes

Un contrôle prévu mais jamais exécuté crée une fausse sécurité et aucune traçabilité. Mieux vaut 5 contrôles réellement exécutés que 15 contrôles théoriques sur le papier.

Pour cela nous vous proposons 3 niveaux d'application pour vos équipes.

- Automatiser plutôt qu'assigner,
- intégrer les contrôles dans les gestes et processus existants,
- Concentre le risque humain sur les 3 véritables points de rupture.

Niveau 1 - Automatique (zéro charge collaborateur)

Le système détecte, alerte, bloque. Personne n'a besoin d'y penser.

#	Contrôle	Mécanisme
1	Alerte toute modification de RIB dans SC, PA, ERP	Notification automatique au responsable dès la sauvegarde
2	Double signataire obligatoire sur virements > seuil	Le virement est techniquement bloqué sans 2ème validation
3	Rapprochement bancaire automatique quotidien	Matching automatique flux bancaire → écritures comptable
4	Alerte virement hors plage horaire de travail ou hors pays	Notification immédiate si le virement est effectué à 3h du matin ou vers l'étranger
5	Blocage création fournisseur sans champ RIB validé	Le formulaire ne peut pas être soumis sans le champ obligatoire renseigné
6	Log automatique de tous les accès sensibles	Trace horodatée de qui a accédé à quoi (tréso, paye, droits admin)
7	Analyse statistique automatique des écritures	Détection automatisée des anomalies et comportements inhabituels

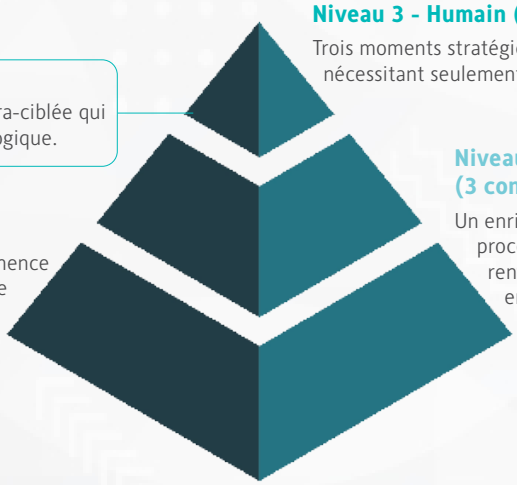
Niveau 2 - Directement intégré aux processus déjà en place

#	Contrôle	Quel process ?	Ce que l'on ajoute concrètement
8	Revue des droits d'accès	Clôture mensuelle (par exemple)	Ajouter un onglet ***« statut droits d'accès »*** dans le dossier de clôture
9	Vérification comptes dormants / fournisseurs inactifs	Revue des tiers en fin de trimestre	Filtre sur les dernières écritures > 1 an
10	Nouvelle mission / nouveau mandat	Paiement des dettes fournisseurs pour le compte des clients	Vérification IBAN par appel avant tout paiement

© - ATH tous droits réservés

Niveau 3 - Humain non-négociable

#	Moment de rupture	Règle absolue	Pourquoi c'est non-négociable ?
11	Changement de RIB d'un fournisseur existant	Appel sur numéro connu (pas celui du mail reçu) pour confirmer	80 % des fraudes au faux fournisseur passent par là
12	Virement exceptionnel > seuil défini	Validation verbale ou SMS par le dirigeant ou DAF, même en déplacement	La fraude au président cible exactement les moments où on ne veut pas déranger
13	Arrivée ou départ d'un collaborateur	Revue immédiate des accès : créer / supprimer / modifier les droits le jour même	40 % des fraudes internes sont commises par d'anciens employés avec des accès non révoqués



Niveau 3 - Humain (3 contrôles critiques)

Trois moments stratégiques jamais délégués nécessitant seulement 2 minutes par événement.

Priorité à l'action directe

Une intervention humaine ultra-ciblée qui complète la vigilance technologique.

Niveau 2 - Intégré (3 contrôles)

Un enrichissement des processus actuels pour renforcer les actions déjà en place.

Niveau 1 - Automatique (7 contrôles)

Un système qui veille en permanence pour assurer une sécurité et une surveillance constantes.

© - ATH tous droits réservés

7 Cybersécurité et protection de données : le socle minimal

a. Ce que toute structure doit mettre en place a minima

MFA sur tous les accès sensibles

Le MFA (authentification à double facteur) consiste à exiger, en plus du mot de passe, une confirmation supplémentaire : un code reçu par SMS, une application d'authentification, une clé physique.

À activer en priorité sur :

- La messagerie professionnelle,
- Le logiciel de facturation,
- Le logiciel comptable,
- La Plateforme Agréée.

Pourquoi c'est primordial : 90 % des compromissions de comptes exploitent un mot de passe seul. Le MFA neutralise cette attaque dans la quasi-totalité des cas.

Gestion des mots de passe

Deux règles suffisent :

- **Un mot de passe unique par service :** réutiliser le même mot de passe partout revient à utiliser la même clé pour son domicile, son bureau et son coffre-fort.
- **Utiliser un gestionnaire de mots de passe :** qui génère et stocke des mots de passe complexes sans effort de mémoire.

Un gestionnaire de mots de passe ne protège pas contre le vol de session via les cookies (une menace croissante portée par les malwares). La vraie protection contre ce risque passe par la sécurisation des postes de travail.

Mises à jour et sauvegardes

- **Mises à jour :** activer les mises à jour automatiques sur tous les postes et logiciels. Les failles exploitées par les rançongiciels ciblent quasi-exclusivement des logiciels non mis à jour.
- **Sauvegardes :** appliquer la règle 3-2-1, 3 copies, sur 2 supports différents, dont 1 hors site (cloud ou support physique externe). Tester la restauration au moins une fois par an.

Une personne responsable, une procédure d'incident

Désigner nominativement un référent sécurité dans la structure : ce n'est pas forcément un technicien, c'est la personne qui sait quoi faire si quelque chose se passe.

Cette personne doit connaître les réponses à ces 3 questions :

- Qui appelle-t-on en cas d'incident ? (Prestataire informatique, numéro d'urgence),
- Quels sont les accès à couper en premier ?
- Où sont les sauvegardes et comment les restaurer ?

Ces 3 réponses doivent être écrites, connues et testées une fois par an. Pas dans la tête d'une seule personne.

© - ATH tous droits réservés

b. Les risques spécifiques à surveiller

Votre Plateforme Agréée est un prestataire qui traite des données financières sensibles pour votre compte.

Quelques questions à poser par écrit :

Questions	Pourquoi c'est important
Êtes-vous immatriculés à la DGFiP ?	Vérification du statut légal
Où sont hébergés les données ? (localisation précise)	Exposition au droit étranger (ex. *Cloud Act Américain*)
Quel est votre plan de continuité en cas d'incident ?	Votre activité dépend de leur disponibilité
Faites-vous l'objet d'audits de sécurité réguliers ?	Exiger les certificats
Quels sont vos délais de notification en cas de violation de données ?	Obligation RGPD : 72h maximum

Si votre Plateforme Agréée ne peut pas répondre à ces questions, c'est un signal d'alerte.

API et interconnexions : les questions à poser

Vous n'avez pas besoin de comprendre techniquement comment fonctionne une API. Vous devez en revanche savoir poser les bonnes questions à votre prestataire ou DSI :

Questions	Réponses
Qui a accès aux clés API de nos connexions ?	La liste doit être courte et nominative
Les clés API sont-elles renouvelées régulièrement ?	Une clé jamais changée est une clé potentiellement compromise sans que vous le sachiez
Que se passe-t-il si l'un de nos prestataires est piraté ?	La réponse révèle leur niveau de préparation
Pouvez-vous me montrer la liste des applications qui ont accès à nos données comptables ?	Cette liste doit être revue au moins 2 fois par an

© - ATH tous droits réservés

Logs et preuves : le minimum légalement exploitable

En cas de fraude avérée, la première question de votre avocat ou de la police sera :

« *Avez-vous des traces de ce qui s'est passé ?* » Sans logs, pas de preuve. Sans preuve, pas de recours.

Ce que vous devez avoir *a minima* :

- **Le journal de connexion sur vos outils sensibles :** qui s'est connecté, quand, depuis qu'elle adresse IP, activé dans les paramètres de la plupart des logiciels, gratuitement.
- **L'historique des modifications :** qui a modifié quoi dans la fiche fournisseur, dans les paramètres bancaires, dans les droits d'accès.
- **La durée de conservation :** 1 an minimum, 3 ans recommandé pour les données fiscales.

Règle pratique : Si votre logiciel ne génère pas de logs, c'est un critère à intégrer dans votre prochain appel d'offres. En 2026, l'absence de traçabilité n'est plus acceptable pour un outil traitant des données financières.

Synthèse

Niveaux	Ce qu'il faut faire	Délais
Socle minimal	MFA + mots de passe + sauvegardes + référent	24h - 48h
Intermédiaire	Audit PA + revue API + activation des logs	1 à 2 semaines
Avancé	Tests de restauration + revue annuelle des accès + clauses contractuelles	Processus continu

Le risque zéro n'existe pas. L'enjeu est de rendre l'attaque moins rentable pour le fraudeur et de disposer des éléments nécessaires pour comprendre et documenter ce qui s'est produit si elle aboutit malgré tout.

© - ATH tous droits réservés

8 Et maintenant que faire ?

Vous avez lu ce guide jusqu'ici. Vous avez probablement reconnu des situations, identifié des angles morts, peut être noté quelques actions à mener.

La question qui reste est simple : **par où commencer ?**

Un diagnostic

01 Vos processus de paiement résistent-ils à un scénario de fausse facture ?

- Avez-vous une procédure écrite de vérification des IBAN avant tout nouveau paiement ?
- Vos collaborateurs savent-ils quoi faire s'ils reçoivent une demande de changement de coordonnées bancaires par email ?

02 Vos accès numériques sont-ils sous contrôle ?

- Le MFA est-il activé sur votre messagerie, votre logiciel comptable, votre banque en ligne ?
- Avez-vous la liste des personnes qui ont accès à vos outils financiers et cette liste est-elle à jour ?

03 Savez-vous ce que fait votre Plateforme Agréée avec vos données ?

- Connaissez-vous le nom de votre ou de vos Plateforme(s) Agréée(s) ?
- Avez-vous signé un contrat qui précise où sont hébergées vos factures et comment elles sont protégées ?

04 Vos équipes reconnaîtraient-elles un signal d'alerte ?

- Vos collaborateurs ont-ils été sensibilisés aux fraudes documentées dans ce guide ?
- Existe-t-il un réflexe collectif, pas seulement individuel, face à une demande inhabituelle ?

05 En cas d'incident, sauriez-vous quoi faire dans les premières heures ?

- Avez-vous un référent identifié ?
- Avez-vous des traces exploitables de vos transactions et connexions récentes ?

© - ATH tous droits réservés

Ce que vos réponses révèlent

Vous avez répondu oui à toutes les questions

Votre dispositif est solide. L'enjeu est maintenant de le maintenir dans la durée. Les fraudes évoluent, vos outils et vos équipes aussi. Une revue annuelle suffit généralement à rester à niveau.

Vous avez répondu non à une ou deux questions

Vous avez des angles morts identifiés. La bonne nouvelle : ils sont connus, donc traitables. La priorité est de ne pas les laisser ouverts trop longtemps, un angle mort connu et non traité est plus dangereux qu'un angle mort ignoré, parce qu'il crée un faux sentiment de maîtrise.

Vous avez répondu non à trois questions ou plus

Votre exposition au risque est réelle et probablement sous-estimée. Ce n'est pas un jugement, c'est le cas de la majorité des structures qui n'ont pas encore eu le temps de structurer ce sujet. La réforme de la facturation électronique accélère l'urgence : les nouvelles interconnexions qu'elle crée ouvrent des portes avant que les verrous soient posés.

La prochaine étape concrète

Quel que soit votre profil, la même logique s'applique :

Ce qui est nommé peut-être traité. Ce qui est mesuré peut-être amélioré.

Ce guide vous a donné les mots et les repères. La prochaine étape est de les appliquer à votre situation spécifique, vos outils, vos flux, vos équipes, vos clients.

C'est précisément ce que nous mettons en place avec nos clients : transformer une prise de conscience en dispositif concret, adapté à la réalité de leur organisation, sans complexité inutile.

© - ATH tous droits réservés

Toute reproduction, intégrale ou partielle, faite sans le consentement de l'éditeur, est illicite. Seules sont autorisées les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective d'une part et, d'autre part, les analyses et courtes citations dans un but d'exemple et d'illustration (art. L.122-4, L.122-5 et L.335-2 du Code de la propriété intellectuelle).

Des photocopies payantes peuvent être réalisées avec l'accord de l'éditeur.

S'adresser au : Centre français d'exploitation du droit de copie - 16, rue du Quatre Septembre - CS 46354 - 75082 PARIS CEDEX 2 - Tél. 01 44 07 47 70.

Nexia S&A regroupe 600 professionnels dont 60 associés au service de 5000 clients, ETI et PME, en audit, expertise comptable, transactions services, conseil financier et gestion sociale.

Contactez-nous

T: 01 47 66 77 88
contact@nexia-sa.fr

nexia-sa.fr