Fraude au virement et cybersécurité : le guide pratique de l'étude notariale

Inclus : deux guides de bonnes pratiques de sécurité à remettre à vos collaborateurs et à vos clients

La confiance ne se transmet pas par e-mail. Fraude au virement et usurpation d'identité, le plus souvent ouvertes par un hameçonnage (phishing) : un guide pratique pour protéger l'étude et ses clients, à l'heure où la responsabilité du notaire se joue aussi sur le canal de transmission.

Une boîte de messagerie d'étude contient presque tout ce qu'un escroc peut espérer : les dates de signature, les montants à virer, l'identité des parties, les échanges avec la banque et, trop souvent encore, le relevé d'identité bancaire de l'office. Le notaire manie des fonds importants et inspire une confiance que personne ne songe à remettre en cause. C'est précisément ce qui fait de l'étude une cible : le fraudeur n'a pas besoin de forcer un coffre, il lui suffit d'emprunter la voix de l'étude au bon moment.

Les Notaires de France multiplient les alertes depuis plusieurs années. Ce guide en tire les conséquences pratiques : comment opèrent les deux fraudes les plus courantes et la porte d'entrée qu'elles partagent le plus souvent, quelles règles simples l'étude peut adopter dès demain, que faire dans l'heure qui suit un incident, et ce que les outils peuvent apporter sans se substituer à la vigilance de chacun.

Ce que 2026 a mis en lumière

Le 3 septembre 2026, une enquête du *Monde*, fondée sur des documents internes de l'ANSSI et du Conseil supérieur du notariat, a révélé l'ampleur d'une campagne de piratage menée à partir de décembre 2022. Plus de 500 offices, soit environ 7 % de la profession, auraient été compromis, ainsi que le CSN lui-même. Fin 2024, l'ANSSI estimait entre 35 et 40 millions d'euros le montant des virements détournés, en précisant que cette estimation était basse. Selon la même enquête, un document piégé envoyé en mars 2024 depuis un office compromis a atteint plus de dix mille destinataires, et environ 80 % d'entre eux auraient cliqué. Aucun faux acte authentique n'a été identifié, mais l'ANSSI en a sérieusement envisagé le risque.

La même année, un jugement a déplacé la question de la responsabilité. Le 25 mars 2026, le tribunal judiciaire de Paris s'est prononcé sur une vente de 2022. Le notaire avait adressé par courriel le décompte et le RIB de l'étude à l'acquéreur ; le message a été intercepté, le RIB remplacé, et 96 400 € ont été virés sur le compte d'un tiers. Une partie des fonds a pu être récupérée, mais le préjudice restant s'élevait à 68 607,38 €.

> **Ce que le tribunal a retenu.** Le notaire supporte 70 % du préjudice, soit 48 025,17 € : il a transmis le RIB par un courriel non sécurisé et sans mise en garde, alors que la chambre des notaires recommandait dès mars 2022 de ne jamais procéder ainsi. Le tribunal relève aussi qu'il n'a communiqué les éléments permettant de vérifier le compte de l'étude à la Caisse des dépôts qu'après la fraude. L'acquéreur conserve 30 % du préjudice, l'adresse de l'expéditeur frauduleux étant visiblement différente. Les deux banques sont mises hors de cause, les faits étant antérieurs à l'entrée en vigueur de la vérification du bénéficiaire.
>
> *TJ Paris, 11e ch. 2e sect., 25 mars 2026, RG 23/11725, jugement rendu en premier ressort.*

Une décision de première instance ne fait pas jurisprudence, mais son raisonnement mérite l'attention de toute la profession : la vigilance attendue du client n'exonère pas l'étude, et le canal par lequel circule un RIB fait désormais partie de l'analyse.

Deux fraudes, une même porte d'entrée

Les deux fraudes qui touchent le plus souvent les études, la fraude au virement et l'usurpation d'identité, commencent le plus souvent au même endroit : la messagerie. Une boîte compromise sert à la fois à observer, à usurper et à propager.

La porte d'entrée : l'hameçonnage (phishing)

C'est le plus souvent le premier maillon de la chaîne. Un courriel plausible, une facture, un « projet d'acte » ou une notification de partage, et un clic suffit à livrer des identifiants ou à installer un logiciel espion. L'épisode de mars 2024 montre qu'aucune étude n'est à l'abri : le message provenait d'un office bien réel, et la grande majorité des destinataires l'a ouvert. Ce type d'attaque exploite l'attention des personnes plus que les failles des machines ; c'est donc d'abord par les personnes que passe la défense.

La fraude au virement

C'est la plus fréquente et la plus coûteuse. Le fraudeur prend le contrôle d'une messagerie, celle de l'étude, du client, de l'agent immobilier ou du banquier, et y reste parfois plusieurs semaines sans se manifester. Il suit le dossier, attend l'appel de fonds, intercepte le message qui contient le RIB, modifie les coordonnées dans la pièce jointe et le renvoie depuis une adresse presque identique. La campagne révélée en 2026 a aussi recouru à la fraude dite « au président » : l'escroc se fait passer pour un notaire afin d'obtenir d'un confrère ou d'un partenaire un virement urgent. Les Notaires de France signalent enfin de faux conseillers bancaires qui s'immiscent dans le projet immobilier pour détourner l'apport du client.

L'usurpation d'identité

Elle joue dans les deux sens. Vers l'extérieur, l'escroc emprunte l'identité de l'étude : faux courriels, faux numéros, faux notaires qui contactent des héritiers ou des acquéreurs. Vers l'intérieur, il se présente à l'étude sous une identité qui n'est pas la sienne : faux vendeur d'un bien qu'il ne possède pas, faux héritier, pièces d'identité ou avis d'imposition falsifiés, que les outils numériques rendent chaque année plus crédibles. Dans les deux cas, c'est la confiance attachée à l'acte authentique qui est exploitée.

> **Nota bene.** L'hameçonnage n'est pas la seule porte d'entrée. D'autres voies, moins courantes, existent : l'appel d'un faux conseiller bancaire ou d'un faux confrère, un SMS frauduleux, des pièces falsifiées présentées directement à l'étude, ou encore l'intrusion par un poste mal protégé ou un accès à distance non sécurisé.

> *Le fraudeur n'a pas besoin de forcer la porte de l'étude. Il lui suffit de lire son courrier et d'attendre le bon moment.*

Le guide pratique : sept règles pour l'étude

Aucune de ces règles n'exige d'investissement lourd. Leur efficacité tient à leur application systématique, par tous, sur tous les dossiers.

1. **Aucun RIB par courriel simple.** Ni envoyé, ni reçu. Les coordonnées bancaires circulent par un canal sécurisé, avec authentification du destinataire, ou sont remises en main propre.
2. **Prévenir le client dès l'ouverture du dossier.** Par écrit, avant tout appel de fonds : le compte de l'étude est tenu par la Caisse des dépôts (BIC CDCGFRPPXXX), jamais par une banque étrangère ; les adresses de l'étude se terminent par notaires.fr ; l'étude ne modifiera jamais ses coordonnées bancaires en cours de dossier. C'est précisément la mise en garde dont l'absence a été reprochée en 2026.
3. **Rappeler, toujours, à un numéro connu.** Tout changement de coordonnées bancaires, qu'il vienne d'un client, d'un vendeur, d'un héritier ou d'un confrère, est confirmé par téléphone, au numéro qui figure déjà au dossier et jamais à celui indiqué dans le message.
4. **Deux validations pour tout virement sortant.** Aucun décaissement n'est ordonné par une seule personne. Un RIB nouveau, modifié ou domicilié à l'étranger déclenche un contrôle renforcé, quelle que soit l'urgence invoquée.
5. **Verrouiller les accès.** Double authentification sur la messagerie et les accès à distance, comptes nominatifs, mises à jour appliquées sans délai, audit régulier. Selon les documents de l'ANSSI cités par *Le Monde*, la moitié des études n'avaient jamais fait auditer leur informatique.
6. **Contrôler l'identité, sans exception.** Pièces en original, cohérence entre l'identité, le titre et les coordonnées, prudence redoublée face à toute demande urgente, inhabituelle ou présentée comme confidentielle, y compris lorsqu'elle semble venir d'un confrère.
7. **Former toute l'équipe, accueil compris.** Les fraudes réussies exploitent rarement une faille technique isolée ; elles exploitent une habitude. Une courte session par semestre, nourrie de cas concrets, vaut mieux qu'une charte que personne ne relit.

Dans l'heure qui suit une fraude

- Appeler sans attendre la banque émettrice pour demander le rappel des fonds : chaque heure compte.
- Prévenir par téléphone le client et, le cas échéant, le confrère ou la banque concernés.
- Couper les accès compromis, changer les mots de passe, conserver les messages et leurs en-têtes comme preuves.
- Déposer plainte et se faire orienter sur 17cyber.gouv.fr, le guichet d'assistance de la police, de la gendarmerie et de Cybermalveillance.gouv.fr.
- Si des données personnelles ont été exposées, notifier la CNIL au plus tard 72 heures après en avoir pris connaissance (article 33 du RGPD).
- Informer l'assureur de responsabilité civile professionnelle et la chambre.

GRATUIT · VERSION IMPRIMABLE

Pour l'équipe de l'étude. Ces règles existent en code pratique complet recto verso (deux exemplaires par feuille A4), avec les signaux d'alerte et la conduite à tenir en cas de fraude, à afficher sur chaque bureau et à remettre à chaque collaborateur. Pour le recevoir gratuitement en PDF imprimable, écrivez-nous à **info@beehavesoft.com** avec pour objet « Flyer bonnes pratiques de sécurité pour l'étude ». Pour un guide à l'image de l'étude, indiquez dans votre e-mail ses coordonnées et joignez son logo : nous le personnalisons pour vous.

GRATUIT · VERSION IMPRIMABLE

Pour les clients de l'étude. Une carte recto verso, à découper et à plastifier, reprend les vérifications à faire avant tout virement, avec un emplacement pour le cachet et le téléphone de l'étude. Pour la recevoir gratuitement en PDF imprimable, écrivez-nous à **info@beehavesoft.com** avec pour objet « Flyer bonnes pratiques de sécurité pour les clients de l'étude ». Pour une carte à l'image de l'étude, indiquez dans votre e-mail ses coordonnées et joignez son logo : nous la personnalisons pour vous.

Les deux versions imprimables peuvent aussi être demandées depuis notre page conseils : **www.beehave.work/beehave-conseils-securite-etudes**

Ce que les outils apportent, et ce qu'ils ne remplacent pas

Depuis le 9 octobre 2025, le règlement européen sur les virements instantanés impose aux banques de vérifier, avant chaque virement, que le nom du bénéficiaire correspond à l'IBAN saisi. Cette vérification du bénéficiaire est un progrès réel. Elle a toutefois ses limites : elle signale une discordance sans interdire au client de passer outre, elle intervient au tout dernier moment, et elle ne dit rien de la manière dont le RIB est parvenu au client. La question du canal reste entière, et c'est elle que le tribunal de Paris a examinée.

C'est sur ce canal qu'agit Beesafe, le module d'échange sécurisé de Beehave. Il permet d'envoyer, de recevoir et d'échanger des documents, RIB compris mais pas seulement, dans un espace protégé par double authentification plutôt qu'en simple pièce jointe. L'interface est multilingue, ce qui compte pour les clients et les héritiers établis à l'étranger, et personnalisable. Beesafe se synchronise avec le logiciel de rédaction d'actes pour récupérer automatiquement les coordonnées des clients et des confrères (adresse électronique, téléphone, adresse postale) : aucune coordonnée n'est ressaisie, ni recopiée depuis un message qui pourrait avoir été falsifié. Enfin, les échanges peuvent être effacés automatiquement au terme d'une durée fixée par l'étude, six mois par défaut, ce qui limite la conservation des données au strict nécessaire, dans l'esprit du RGPD. Beesafe s'utilise intégré à Beehave Notaires ou comme module autonome, et les données sont hébergées en France.

Un canal sécurisé ne protège rien si l'on accepte, par ailleurs, un changement de RIB annoncé par courriel. Mais il retire au fraudeur son terrain favori.

La sécurité commence par un vrai outil de CRM

À y regarder de près, la plupart de ces fraudes exploitent une même faiblesse : une coordonnée douteuse que personne n'est en mesure de vérifier. Un numéro de téléphone recopié depuis un courriel, une adresse qui diffère d'une lettre, un RIB que l'on croit déjà connaître. Une étude qui dispose, pour chaque client et chaque confrère, d'une fiche unique, à jour et partagée par toute l'équipe, se donne le moyen le plus simple de déjouer ces manœuvres : comparer.

C'est le socle de Beehave Notaires. La plateforme vient en complément de votre logiciel de rédaction d'actes, avec lequel elle se synchronise, sans double saisie : une vue à 360° de vos dossiers, le pilotage de la charge de votre équipe, et NotaCRM, son module CRM taillé pour le notariat, capable de segmenter votre clientèle et de déclencher les bonnes actions au bon moment. Beehave, qui cumule plus de cinq ans d'expérience dans l'automatisation des études notariales, la conçoit autour d'un principe simple : une donnée fiable protège l'étude autant qu'elle sert la relation client.

Références

- *Le Monde*, enquête du 3 septembre 2026 sur le piratage du notariat (chiffres de l'ANSSI cités par le quotidien).
- Tribunal judiciaire de Paris, 11e ch. 2e sect., 25 mars 2026, RG 23/11725.
- Notaires de France, « Fraude au RIB : hausse des arnaques » (11 mars 2022), « Fraude au virement ou au RIB : les Notaires de France appellent à la vigilance » et « Cybermalveillance : prévention et conseils », notaires.fr.
- Règlement (UE) 2024/886 du 13 mars 2024 relatif aux virements instantanés (vérification du bénéficiaire). Règlement (UE) 2016/679 (RGPD), article 33.
- Cybermalveillance.gouv.fr, fiche réflexe « L'escroquerie aux faux ordres de virement (FOVI) », en partenariat avec le ministère de l'Intérieur et l'ANSSI. Gendarmerie nationale, « Comment se prémunir contre les escroqueries aux faux ordres de virement ? » (mise à jour du 13 août 2024).
- ANSSI, « Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures » et « Recommandations relatives à l'authentification multifacteur et aux mots de passe » (2021).
- 17cyber.gouv.fr, guichet national d'assistance aux victimes de cybermalveillance.

Avertissement. *Ce livre blanc résume les recommandations publiées par les Notaires de France, Cybermalveillance.gouv.fr, la Gendarmerie nationale et l'ANSSI, ainsi qu'une décision de justice rendue en premier ressort. Il est fourni à titre d'information : il ne constitue pas un conseil juridique et ne remplace ni l'analyse de vos propres procédures, ni un audit de sécurité de l'étude, ni l'avis de votre assureur.*

Un RIB juste, au bon destinataire, par le bon canal.

Découvrez comment Beehave Notaires, son CRM NotaCRM et Beesafe sécurisent vos échanges et structurent votre relation client.

Réserver une démonstration **Visiter notre site**

Beehave Notaires — info@beehavesoft.com — www.beehave.work

Les livres blancs Beehave Notaires

Voici quelques-uns de nos livres blancs. Retrouvez la totalité de nos publications, les plus récentes et les plus utiles, sur notre page ressources.

- **Fraude au virement et cybersécurité : le guide pratique de l'étude notariale** *(ce document)*
- **Rédiger n'est pas tout** · intelligence artificielle et relation client
- **La gestion de la relation client (GRC)**
- **L'automatisation des processus métiers (1er volet)**

Retrouvez l'ensemble de nos livres blancs sur beehave.work/ressources →

Et nos conseils de sécurité pour l'étude sur beehave.work/beehave-conseils-securite-etudes →