DÉCRYPTAGE · AUTODÉFENSE

Escroqueries financières : le manuel *d'autodéfense*

Le dossier technique n°23 jugeait des produits légaux et médiocres ; ce dossier traite du crime : faux livrets, faux conseillers bancaires, usurpations d'identité, plateformes fantômes, arnaques sentimentales à la crypto, fraude au président pour les PME. Un demi-milliard d'euros par an au bas mot, des victimes de tous niveaux d'éducation, et des méthodes industrialisées par l'IA. Les sept familles d'attaques, les cinq réflexes qui bloquent 95 % des cas, et quoi faire dans l'heure si c'est déjà trop tard.

SOMMAIRE

01 Le crime, pas la médiocrité : changement de registre

02 Pourquoi vous êtes visé, et pourquoi l'intelligence ne protège pas

03 Famille 1 et 2 : les faux placements et les fausses plateformes

04 Famille 3 : le faux conseiller bancaire, l'arnaque reine

05 Familles 4 et 5 : sentimentale-crypto et « récupération de fonds »

06 Familles 6 et 7 : l'entreprise visée (président, FOVI, factures)

07 L'IA des deux côtés : deepfakes, clonage de voix, et parades

08 Les cinq réflexes qui bloquent 95 % des attaques

09 C'est arrivé : la procédure de la première heure

10 Conclusion · Annexes : chiffres-clés, glossaire, sources

Rédigé par Stéphane Baron, sous la supervision de Bernard Prats-Desclaux. Dossier pédagogique, juillet 2026. Complète le dossier technique n°23 (produits médiocres légaux) : ici, on parle d'infractions. Sources : AMF, ACPR, cybermalveillance.gouv.fr.

1 Le crime, pas la médiocrité

THÈSE — CONTRE L'INDUSTRIE DE LA FRAUDE, LA CULTURE FINANCIÈRE EST UNE ARME, PAS UN VACCIN

≈ 500 M€/an	≈ 1 200+	24-72 h	100 %
DE PRÉJUDICE DÉCLARÉ (ÉPARGNE) : LE RÉEL EST MULTIPLE	SITES AJOUTÉS CHAQUE ANNÉE AUX LISTES NOIRES AMF/ACPR	LA FENÊTRE OÙ L'ARGENT EST ENCORE PARFOIS RÉCUPÉRABLE	DES PROFILS TOUCHÉS : CADRES, DIRIGEANTS ET FINANCIERS COMPRIS

Toute la collection suppose un adversaire légal : des produits chers (dossier technique n°22), des stratégies vendeuses (dossier technique n°23), des biais (dossier technique n°19). Ce dossier change de registre : l'adversaire est un criminel organisé, souvent à l'étranger, industrialisé (centres d'appels, scripts testés, IA), et son produit n'est pas médiocre : il est FAUX. L'AMF et l'ACPR chiffrent le préjudice déclaré en centaines de millions d'euros par an (500 M€ est l'ordre de grandeur bas : la honte fait taire une majorité de victimes), les listes noires s'allongent de plus d'un millier de sites par an, et le profil des victimes détruit le mythe protecteur : cadres, professions libérales, dirigeants, retraités aisés : PLUS le patrimoine est gros, plus la cible est travaillée. Il faut le dire sans détour : votre intelligence ne vous protège pas, car l'attaque ne vise pas l'intelligence : elle vise l'émotion (urgence, peur, confiance, solitude) : le dossier technique n°19 industrialisé par des professionnels. La protection vient des PROCÉDURES : cinq réflexes mécaniques (section 8), les mêmes garde-fous qu'au dossier technique n°19, version sécurité. Ce dossier arme la famille entière : il se partage, notamment avec les parents âgés, cibles préférées de la famille 4.

2 Pourquoi vous êtes visé

LA MÉCANIQUE — UNE INDUSTRIE AVEC SON MARKETING, SES FICHIERS ET SES COMMERCIAUX

Représentez-vous l'adversaire tel qu'il est : une PME du crime, avec acquisition de prospects (fuites de données : chaque piratage de site marchand alimente les fichiers ; formulaires « investissement » sponsorisés sur les réseaux : oui, les plateformes encaissent la publicité des fraudeurs), qualification (le premier appel évalue votre patrimoine, votre solitude, votre appétence : les meilleurs prospects passent aux « closers »), scripts éprouvés (utilisant exactement les biais du dossier technique n°19 : urgence : « l'offre ferme ce soir », autorité : « je suis mandaté par l'AMF », preuve sociale : « vos voisins de [votre ville] ont souscrit », réciprocité : les premiers « gains » affichés), et fidélisation : car l'arnaque moderne ne prend pas tout d'un coup : elle affiche des gains fictifs sur une interface soignée, encaisse vos rechargements, puis invente des « frais de déblocage » jusqu'à l'assèchement : la victime moyenne verse PLUSIEURS fois. Comprendre cette industrialisation change la posture : vous ne faites pas face à un escroc : vous êtes entré dans un tunnel commercial criminel, et la seule victoire est de ne jamais y entrer : d'où la primauté des réflexes d'entrée (section 8) sur la vigilance continue, qui s'érode toujours.

3 Familles 1 et 2 : faux placements, fausses plateformes

LE CLASSIQUE — LE RENDEMENT IRRÉSISTIBLE QUI N'EXISTE PAS

- **Famille 1 · Le faux placement « sûr et rentable » :** faux livrets à 5-8 % (usurpant de vraies banques : plaquettes parfaites, conseillers au téléphone, IBAN… au nom d'une société tierce : LE signal), fausses SCPI (dossier technique n°06 usurpé), faux parkings d'aéroport, EHPAD, vins, forêts, énergies vertes : le sous-jacent suit les modes, la mécanique jamais : rendement au-dessus du marché + garantie affirmée + urgence. Le dossier technique n°23 (fiche 10) fournissait déjà le verdict théorique : au-dessus du taux sans risque (dossier technique n°04 : ~2 %), un rendement « garanti » est structurellement frauduleux ou risqué : ici, il est les deux.
- **Famille 2 · La fausse plateforme de trading/crypto :** sites léchés, comptes de démonstration truqués (vous « gagnez » toujours au début), célébrités deepfakées en vitrine (section 7), et le tunnel de la section 2 : dépôts croissants, gains fictifs, retraits impossibles moyennant « taxes » : la variante moderne du dossier technique n°23 fiche 2, en version pénale. Test d'hygiène systématique : le nom sur REGAFI (agréments bancaires), sur la liste blanche AMF des PSAN pour la crypto, et sur les listes NOIRES AMF/ACPR : trois minutes, gratuites : aucune contrepartie sérieuse n'échoue aux trois.

4 Famille 3 : le faux conseiller bancaire

L'ARNAQUE REINE — LE SPOOFING, OU QUAND VOTRE BANQUE VOUS APPELLE

La fraude qui explose depuis 2022 et fait les plus gros dégâts individuels : vous recevez un appel du numéro AFFICHÉ de votre banque (le « spoofing » d'affichage est techniquement trivial), d'un « conseiller sécurité » calme et professionnel : des opérations suspectes frappent votre compte, il faut URGEMMENT sécuriser : valider des annulations sur votre appli (en réalité : valider des virements), communiquer des codes reçus par SMS, voire virer vous-même vers un « compte sécurisé ». Tout y est : le numéro authentique, vos données réelles (fuites de la section 2 : il connaît votre conseiller, vos dernières opérations), l'autorité, l'urgence, la peur : les victimes incluent des banquiers. La parade tient en UNE règle absolue, à graver : **votre banque ne vous fera JAMAIS valider une opération par téléphone, ni communiquer un code, ni « déplacer » des fonds pour les protéger** : toute demande de

ce type EST la fraude, sans exception. Le réflexe : raccrocher, et rappeler soi-même le numéro officiel (celui de la carte), depuis un AUTRE téléphone si possible (les fraudeurs savent maintenir la ligne ouverte). Point juridique utile : la jurisprudence récente (Cour de cassation, 2023) a renforcé le remboursement des victimes de spoofing par les banques, la négligence grave n'étant plus présumée du seul fait de la validation : déclarer vite et par écrit (section 9) conditionne tout.

5 Familles 4 et 5 : la sentimentale-crypto et la « récupération »

LES PLUS CRUELLES — LE TEMPS LONG DU LIEN, PUIS LA DOUBLE PEINE

— **Famille 4 · L'arnaque sentimentale-investissement** (dite « pig butchering » : l'engraissement) : un contact « accidentel » (réseau social, mauvais numéro), des semaines ou des mois de lien quotidien (amitié, romance : le crime organisé y emploie des opérateurs à temps plein, parfois eux-mêmes victimes de traite en Asie du Sud-Est : l'envers documenté du décor), puis la confidence : « j'investis en crypto, regarde mes gains » : et le tunnel de la famille 2, avec l'ancrage affectif en accélérateur. Préjudices individuels records (souvent > 100 k€), cibles : personnes isolées de tous âges : LA famille d'arnaque dont il faut parler à ses proches, parents âgés en tête : en parler AVANT, car pendant, la victime défend son escroc contre sa famille : c'est le symptôme central.

— **Famille 5 · La « récupération de fonds » :** la double peine industrialisée : les fichiers de victimes se revendent, et des « cabinets » (faux avocats, fausse Interpol, faux régulateurs) contactent les victimes pour récupérer les sommes perdues : contre honoraires d'avance : la victime paie une seconde fois. Règle absolue : AUCUN organisme légitime ne demande d'argent pour récupérer des fonds volés ; les seules voies réelles sont la section 9 : banque, plainte, signalements officiels : gratuites.

6 Familles 6 et 7 : l'entreprise visée

LE VOLET PME — LE DIRIGEANT LECTEUR DE CE DOSSIER EST AUSSI UNE CIBLE PROFESSIONNELLE

Le patrimoine professionnel subit ses variantes dédiées, dopées à l'IA. La **fraude au président** : un « dirigeant » (mail usurpé, désormais voix clonée, bientôt visioconférence deepfakée : des cas à plusieurs millions sont documentés, y compris le célèbre virement de 25 M$ validé en visio truquée à Hong Kong en 2024) ordonne à un comptable un virement urgent et confidentiel : l'attaque exploite la hiérarchie comme la famille 3 exploite la banque. Le **FOVI/changement de RIB** : un « fournisseur » (mail compromis ou imité) signale ses « nouvelles coordonnées bancaires » : les règlements partent chez le fraudeur pendant des semaines. Les **faux supports et rançongiciels** (dossier technique n°10 : la rançon reste le business du bitcoin), les fausses administrations (SIRET, RGPD, registres bidons facturés). Les parades sont organisationnelles, pas technologiques : DOUBLE validation systématique de tout virement nouveau ou modifié (deux personnes, deux canaux), rappel du fournisseur au numéro HISTORIQUE pour tout changement de RIB (jamais celui du mail), procédure écrite affichée en compta (« aucune urgence ne déroge »), et culture d'entreprise où le comptable qui VÉRIFIE un ordre du patron est félicité, jamais rabroué : la fraude au président ne réussit que dans les organisations où l'on n'ose pas rappeler le président.

7 L'IA des deux côtés

2026 — CE QUI A CHANGÉ, CE QUI N'A PAS CHANGÉ

L'IA générative a industrialisé la personnalisation : mails sans fautes (l'ancien détecteur orthographique est mort), sites et documents parfaits en heures, voix clonées sur trois secondes d'échantillon (le « papa, j'ai eu un accident » vocal est opérationnel), visioconférences deepfakées (le cas à 25 M$), et des chatbots qui font du lien sentimental à l'échelle (famille 4 sans limite de personnel). Deux conclusions pratiques. D'abord, les VÉRIFICATIONS DE FORME sont mortes : l'apparence (logo, ton, voix, visage) ne prouve plus RIEN : seules tiennent les vérifications de CANAL (rappeler soi-même un numéro connu, se déplacer, un mot de code familial convenu à l'avance pour les urgences : recommandation à appliquer ce soir avec parents et enfants). Ensuite, la défense s'outille aussi : les banques déploient la détection comportementale (virement inhabituel = friction ajoutée : l'acceptez comme un service), la directive européenne DSP3 renforce la vérification du bénéficiaire (le nom du titulaire du RIB enfin contrôlé), et les navigateurs et opérateurs filtrent mieux : mais l'arbitrage final reste humain, et l'humain sous urgence émotionnelle reste le maillon : la boucle du dossier technique n°19 se referme : les procédures écrites À FROID sont la seule défense qui tienne À CHAUD.

8 Les cinq réflexes qui bloquent 95 % des attaques

LE CŒUR DU DOSSIER — MÉCANIQUES, ENSEIGNABLES, NON NÉGOCIABLES

- **Réflexe 1 · Je ne donne jamais suite à un contact ENTRANT :** tout démarchage financier (appel, mail, réseau social, « conseiller » spontané) meurt à l'entrée : si l'offre m'intéresse, c'est MOI qui rappelle l'institution par son canal officiel. Ce seul réflexe tue les familles 1, 2, 3 et l'essentiel de la 4.
- **Réflexe 2 · Urgence = fraude :** aucune opération patrimoniale légitime n'exige une décision dans l'heure (la collection entière en témoigne : dossier technique n°20 compris). Toute pression temporelle déclenche mon délai de 72 h (dossier technique n°19) et un appel à un tiers de confiance.
- **Réflexe 3 · Je vérifie les registres, trois minutes chrono :** REGAFI (banques), ORIAS (intermédiaires), liste blanche PSAN et listes NOIRES AMF/ACPR : avant tout premier euro. Une contrepartie absente ou blacklistée : terminé, sans appel du 06 pour « s'expliquer ».
- **Réflexe 4 · Le canal indépendant, toujours :** banque qui appelle : je raccroche et rappelle le numéro de ma carte ; fournisseur qui change de RIB : numéro historique ; enfant en détresse vocale : mot de code familial ; patron pressé : double validation. La règle unique : ne jamais vérifier une demande PAR LE CANAL qui l'apporte.
- **Réflexe 5 · Le test du dossier technique n°23, version pénale :** rendement > taux sans risque + garantie + « réservé/urgent/confidentiel » = fraude par définition, même avec un beau site, même recommandé par une connaissance (dont le compte est peut-être compromis), même « validé » par une célébrité (deepfake). L'espérance ne se discute pas avec un criminel : elle est de −100 %.

9 C'est arrivé : la première heure

PROCÉDURE D'URGENCE — CHAQUE HEURE COMPTE, LA HONTE ATTENDRA

Dans l'ordre, montre en main. **H+0 : la banque** : opposition, demande de RAPPEL DE FONDS (recall) sur les virements : c'est faible en délai > 48 h mais réel avant, surtout si le compte destinataire est en France/SEPA : appeler, PUIS confirmer par écrit daté (la traçabilité conditionne le remboursement de

la famille 3). **H+1 : geler la surface d'attaque** : mots de passe (banque, mail d'abord : le mail compromis rejoue tout), oppositions cartes, et si des documents d'identité ont fui : signalement (le fraudeur ouvrira des comptes à votre nom). **Jour 1 : la plainte** : dépôt (commissariat ou plainte en ligne THESEE pour les escroqueries internet) avec TOUT l'historique (mails, numéros, IBAN, captures : ne rien supprimer) ; signalements parallèles : AMF Épargne Info Service, cybermalveillance.gouv.fr, Pharos, SignalConso selon le cas : chaque signalement alimente les listes qui protègent les suivants. **Semaine 1 : l'écosystème** : déclarer aux impôts le cas échéant (des déductions de pertes existent dans certains cas), prévenir les proches (votre carnet d'adresses est peut-être la prochaine cible), et REFUSER tout contact « récupérateur » (famille 5 : ils arrivent dans le mois). Enfin, le plus important humainement : en parler : à la famille, au médecin si le choc est rude : les victimes se murent, les fraudeurs comptent dessus, et la parole est ce qui protège les autres : il n'y a AUCUNE honte à avoir été attaqué par des professionnels : il y en aurait à laisser le silence les servir.

10 Conclusion

La fraude financière est la seule classe de « produits » dont l'espérance est certaine : −100 %, plus les frais de la récupération fantôme. Contre son industrialisation, dopée à l'IA, la culture financière de cette collection aide (qui connaît le taux sans risque du dossier technique n°04 rit au nez du livret à 8 %) mais ne suffit pas : la défense réelle est procédurale : cinq réflexes mécaniques, appris à froid, appliqués sans exception, et transmis autour de soi comme on transmet les gestes qui sauvent : ce dossier est fait pour être partagé, jusqu'à la table familiale du dimanche. Le dossier technique n°19 l'a établi pour les marchés, ce dossier le répète pour le crime : on ne négocie pas avec son cerveau sous urgence émotionnelle : on lui a préparé des rails. Dernier dossier de la vague, et synthèse de toute la collection : construire son allocation.

A Annexe · Chiffres-clés

DONNÉE	VALEUR	SOURCE
Préjudice « épargne » déclaré en France	**≈ 500 M€/an (sous-déclaré)**	AMF/ACPR/Parquet de Paris, ordres de grandeur
Ajouts annuels aux listes noires	**> 1 200 sites/entités**	AMF-ACPR (assurance-epargne-info-service)
Deepfake record documenté (fraude au président)	**≈ 25 M$ (Hong Kong, visioconférence truquée, 2024)**	Presse internationale
Jurisprudence spoofing	**Cass. com. 2023 : remboursement renforcé, négligence grave non présumée**	Cour de cassation
Fenêtre utile du rappel de fonds	**24-72 h (décroissante)**	Pratique bancaire SEPA
Registres de vérification	**REGAFI · ORIAS · listes blanches PSAN · listes noires AMF/ACPR**	Officiels, gratuits
Plainte en ligne (escroqueries internet)	**THESEE (service-public.fr)**	Ministère de l'Intérieur

B Annexe · Glossaire

Spoofing : falsification du numéro appelant (ou de l'expéditeur) : l'affichage ne prouve rien.

Phishing / smishing / quishing : hameçonnage par mail / SMS / QR code.

Pig butchering : arnaque au lien long (sentimental/amical) débouchant sur un faux investissement.

Fraude au président / FOVI : faux ordre de virement par usurpation du dirigeant / du fournisseur (changement de RIB).

Deepfake / clonage vocal : imitation synthétique du visage ou de la voix : tue la vérification « de forme ».

Recall (rappel de fonds) : demande interbancaire de retour d'un virement frauduleux : efficace tôt, aléatoire ensuite.

Listes noires AMF/ACPR : registres publics des sites et entités identifiés comme frauduleux.

THESEE / Pharos / cybermalveillance.gouv.fr : plainte en ligne / signalement de contenus / assistance officielle.

Arnaque à la récupération : seconde fraude ciblant les victimes de la première contre « honoraires » : aucun organisme légitime ne fait payer une récupération.

Mot de code familial : phrase convenue vérifiant l'identité dans les urgences vocales : la parade au clonage de voix.

C Annexe · Sources

AMF / ACPR : Épargne Info Service, listes noires, mises en garde et bilans annuels ; Parquet de Paris (JUNALCO) : estimations de préjudice.

cybermalveillance.gouv.fr (fiches réflexes) ; THESEE ; Cour de cassation (jurisprudence spoofing, 2023) ; presse internationale (deepfake Hong Kong 2024) ; enquêtes sur les centres de fraude d'Asie du Sud-Est (ONU/ONG).

L'Investisseur Stratège : dossier technique n°10 (rançons), dossier technique n°23 (le légal médiocre : la frontière), dossier technique n°19 (les biais exploités), dossier technique n°04 (le taux sans risque comme détecteur).

Avertissement. Document informatif et pédagogique. En cas de fraude avérée ou suspectée : banque, dépôt de plainte et signalements officiels immédiats ; ne payez jamais un « récupérateur de fonds ». *© 2026 L'Investisseur Stratège · investisseur.strategе@norvalgroup.com*