Dossier

Par ***Éric Allermoz***

Arnaques bancaires, faux sites administratifs, escroqueries sentimentales, désinformation médicale… Les tentatives de manipulation se multiplient dans notre quotidien numérique. Alimentées par nos données personnelles et renforcées par l'intelligence artificielle, elles brouillent toujours davantage la frontière entre le vrai et le faux. Comment les repérer, s'en protéger et réagir si l'on est victime ?

Manipulation en ligne : comprendre pour mieux se protéger

Arnaques et désinformation : l'ère de la manipulation

Ils se font passer pour des notaires, des conseillers, des agents de Sécurité sociale… mais ce sont des escrocs. Malgré la médiatisation du phénomène, le nombre de victimes est en forte hausse.

Selon une étude du Crédoc publiée en février 2026, quatre Français sur dix ont été victimes de cybermalveillance au cours de l'année écoulée. Ces arnaques prennent des formes multiples : un SMS invitant à cliquer sur un lien pour affranchir un colis, une publicité promettant de fructueux rendements en cryptomonnaie, des sites administratifs ultracrédibles… Sans oublier la fraude aux sentiments, qui consiste à soutirer de l'argent à une personne rencontrée en ligne en lui faisant croire à une histoire amoureuse. À chaque fois, le procédé repose sur la manipulation psychologique. En se faisant passer pour un tiers de confiance, les escrocs cherchent à soutirer mots de passe, données personnelles et coordonnées bancaires.

47 %

des Français déclarent avoir été confrontés à une fausse information concernant une question de santé, en 2024. *Verian en partenariat avec l'Inserm (pour Harmonie Santé)*

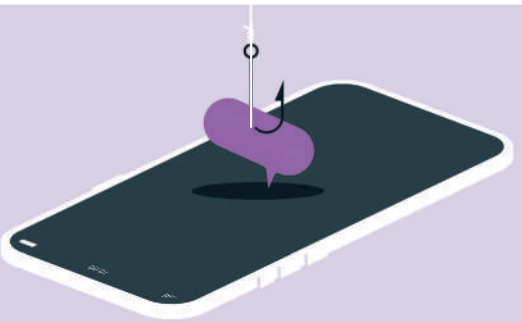
→

Des conséquences financières et psychologiques
Et les conséquences sont lourdes. Selon une étude, menée par Opinium pour le compte du géant des paiements Visa, les victimes d'arnaques en ligne en France ont perdu l'an dernier 147 euros en moyenne, soit un coût de 486 millions d'euros par an pour l'économie tricolore. Dans la plupart des cas, les cybercriminels ne sont pas retrouvés, les victimes rarement indemnisées. Les dégâts dépassent le portefeuille : 41 % des victimes rapportent un impact psychologique durable.

La désinformation en santé : un danger plus insidieux
Aux arnaques financières s'ajoute un autre péril : la désinformation en santé. Amplifiée par les réseaux sociaux *via* des influenceurs depuis la crise du Covid-19, elle détourne certains patients de soins, provoque des retards de diagnostic et nourrit une défiance durable envers la science. Les fake news les plus dangereuses sont celles qui poussent à s'éloigner de la médecine conventionnelle : abandonner une chimiothérapie, rejeter un vaccin, acheter une « solution miracle » au mieux inefficace et au pire dangereuse… Et parfois, c'est une porte d'entrée dans des groupes à dérives sectaires. La santé et le bien-être étaient ainsi en tête des signalements effectués auprès de la Mission interministérielle de lutte contre les dérives sectaires (Miviludes) en 2024.

Les données comme carburant
Arnaques et désinformation partagent les mêmes accélérateurs. D'abord, la masse de données personnelles que nous disséminons au fil de notre vie numérique. Les réseaux sociaux jouent ici un rôle central : Facebook, Instagram, YouTube, WhatsApp et TikTok sont les principales plateformes utilisées pour identifier et approcher les cibles. Les escrocs utilisent également les informations issues de fuites massives de données. Désormais, l'intelligence artificielle est aussi largement mobilisée. En permettant désormais d'imiter la voix ou le visage d'un proche, de générer des textes et des vidéos truquées d'un réalisme troublant, elle offre aux escrocs comme aux désinformateurs des outils d'une puissance inédite. Distinguer le vrai du faux devient alors un défi quotidien.

Faux conseiller, vrai danger



La fraude au faux conseiller bancaire reste l'une des escroqueries les plus répandues.
Le scénario est toujours le même : un escroc usurpe le numéro de téléphone d'une banque, prétend qu'un débit frauduleux est en cours et que des mesures urgentes s'imposent. En réalité, il cherche à faire valider des virements à son profit.
Les mutuelles* ne sont pas épargnées par le phénomène. Le contact téléphonique est souvent précédé d'un hameçonnage par SMS ou d'une publicité en ligne, qui permet à l'escroc de disposer de suffisamment d'informations pour paraître crédible. Par ailleurs, les escroqueries au faux placement financier (des opérateurs promettent des rendements miraculeux pour convaincre leurs victimes d'investir dans des projets inexistants) ont progressé de 277 % en 2025.

*** BPCE Mutuelle ne vous appellera jamais pour vous demander des informations personnelles pour accéder à votre espace personnel.**

Les bons réflexes qui vous protègent

Les escroqueries en ligne et la désinformation ont beau se sophistiquer, elles ne sont pas une fatalité. Face à ces menaces, la meilleure défense reste une combinaison de bons réflexes techniques et intellectuels.

Le premier réflexe à adopter est aussi le plus simple : toujours vérifier la source d'un message avant d'agir. L'adresse e-mail de l'expéditeur est-elle vraiment celle de votre banque ou de l'Assurance Maladie ? Le lien dans le SMS renvoie-t-il bien vers un site officiel ? Le proche qui vous demande de l'argent en urgence est-il vraiment celui qu'il prétend être ? Ces questions prennent quelques secondes et peuvent éviter de lourdes conséquences. Avant d'acheter un produit, vérifiez les avis clients (sur un moteur de recherche, et non sur le site de vente) et le mode de paiement demandé.

La règle d'or : Ne jamais agir dans l'urgence. Si un message vous presse de cliquer, de payer ou de rappeler immédiatement, c'est précisément le moment de marquer une pause. Et si la promesse est démesurée par rapport à l'effort demandé (offre d'investissement extrêmement rentable, remède miracle, produit de qualité vendu très peu cher), redoublez de méfiance.

Protéger ses données

Les données personnelles sont le carburant des arnaques modernes. Les protéger commence par des mots de passe robustes, et surtout différents pour chaque compte. Pour cela, vous pouvez recourir à un gestionnaire de mots de passe, une sorte de coffre-fort numérique qui stocke et génère automatiquement vos identifiants. La Commission nationale de l'informatique et des libertés (Cnil) conseille d'activer la double authentification dès qu'elle est proposée : si quelqu'un tente de se connecter à votre compte depuis un appareil inconnu, vous en êtes immédiatement alerté par SMS ou par e-mail.
Sur les réseaux sociaux, il est recommandé de restreindre au maximum ce qui est visible publiquement : date de naissance, numéro de téléphone, lieu de résidence. Pour les téléphones mobiles, devenus des cibles privilégiées, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) préconise de mettre régulièrement à jour le système d'exploitation et les applications, de ne jamais connecter son appareil à un chargeur ou à un réseau Wi-Fi inconnu, et de bien séparer usages personnels et professionnels.

Cultiver son esprit critique

Avant de suivre un conseil de santé trouvé en ligne, il convient de s'interroger. Qui le produit ? Sur quelle base scientifique ? Un influenceur, même suivi par des millions de personnes, n'est pas une source médicale fiable. Un témoignage individuel, aussi touchant soit-il, ne vaut pas une étude clinique.
Les auteurs du rapport remis au ministère en janvier 2026 sur la désinformation en santé insistent sur une compétence clé : savoir distinguer une opinion ou une croyance d'un fait scientifique établi. Cela implique de comprendre comment se construit une preuve médicale (par des études reproductibles, évaluées par des pairs) et d'identifier les sources fiables : sociétés savantes, Haute Autorité de santé (HAS), revues médicales reconnues, ordres médicaux… En cas de doute, le réflexe le plus sûr reste d'en parler à son médecin.
Les experts recommandent également de se méfier des contenus jouant sur la peur ou l'espoir – deux émotions particulièrement exploitées dans le domaine de la santé – et de ne jamais partager une information avant de l'avoir vérifiée.

Retrouvez tous les conseils de la Cnil pour se protéger en ligne :

« Ces attaques sont menées *via* notre système cognitif »

Antony Dalmiere
Doctorant au LAAS-CNRS

Trois questions à Antony Dalmiere, doctorant au LAAS-CNRS, spécialiste des mécanismes psychosociaux à l'œuvre dans les attaques numériques.

Les arnaques en ligne ne touchent-elles que des personnes naïves ?

Pas du tout ! Ces attaques sont majoritairement menées *via* notre système cognitif. Face à une information, notre cerveau effectue un double traitement : le premier est heuristique (rapide, en surface) ; le second est systématique, c'est celui qui nous permet de réfléchir en profondeur et d'exercer notre esprit critique. Toutes les techniques utilisées par les escrocs visent à ne faire fonctionner que les facultés heuristiques de la victime.

Quels sont les ressorts psychologiques les plus fréquemment exploités ?

Plusieurs stratégies reviennent régulièrement dans les messages frauduleux. Il y a d'abord ce qu'on appelle « l'appâtage » : une promesse amoureuse ou financière destinée à capter l'attention. Il y a aussi la pression temporelle, très efficace, qui oblige à réagir vite sans laisser le temps de réfléchir. Ou encore la technique du « pied dans la porte » : on commence par une demande anodine avant d'en formuler une plus engageante. Sans oublier l'autorité et la peur, deux déclencheurs émotionnels puissants. La difficulté, c'est qu'en être conscient ne suffit pas toujours à s'en prémunir.

L'intelligence artificielle change-t-elle fondamentalement la donne ?

Elle amplifie les mêmes mécanismes de façon radicale. Pendant longtemps, le phishing* se voyait : fautes d'orthographe, tournures bancales, adresses suspectes… Les modèles génératifs ont effacé ces signaux faibles. Les deepfakes [faux enregistrement hyperréaliste d'une personne, NDLR] restent relativement rares, mêmes s'ils sont très médiatisés. Mais la tendance est claire : plus ciblées, plus crédibles, plus rentables, les arnaques changent d'échelle. C'est pour cela qu'au LAAS-CNRS, nous travaillons sur des analyses des procédés de manipulation, qui servent ensuite à entraîner des modèles d'intelligence artificielle capables de les détecter automatiquement.

** Le fait de se faire passer pour un organisme connu pour inciter la victime à transmettre des données personnelles et/ou bancaires.*

Victime ? Voici comment réagir

En cas d'arnaque, les premiers réflexes sont cruciaux. Faites opposition immédiatement auprès de la banque si vos coordonnées bancaires ont été communiquées ou si des débits frauduleux ont été effectués. Contactez également l'organisme usurpé (banque, opérateur, Assurance Maladie) pour les informer et vérifier l'étendue des dégâts. Changez sans attendre tous vos mots de passe compromis, ainsi que ceux des autres comptes sur lesquels vous utilisez le même identifiant. Enfin, conservez toutes les preuves : messages reçus, captures d'écran, historique de navigation. Elles seront indispensables pour la suite des démarches.

48 %
des internautes victimes en 2025 ont entamé des démarches auprès des autorités compétentes, contre 33 % en 2023.
Crédoc (février 2026)

Des outils pour signaler

Plusieurs plateformes permettent de signaler rapidement une arnaque et de protéger d'autres victimes potentielles. Si vous avez reçu un e-mail suspect, signalez-le sur Signal Spam (signal-spam.fr), associé à la Cnil pour identifier et bloquer les principaux émetteurs de spams. Si le message est arrivé par SMS, transférez-le au 33 700. Face à un site frauduleux, signalez son adresse sur Phishing Initiative (phishing-initiative.fr), qui se chargera de le bloquer. Pour tout conseil sur les démarches à suivre, la plateforme Info Escroqueries du ministère de l'Intérieur est joignable gratuitement au 0 805 805 817.

Porter plainte, une démarche essentielle

Même si l'auteur de l'arnaque est anonyme, il est important de porter plainte. Elle permet d'enclencher une enquête, d'alimenter les statistiques (qui orientent les moyens policiers), et constitue souvent un préalable indispensable à toute procédure d'indemnisation.

La voie la plus simple est la plateforme THESEE (traitement harmonisé des enquêtes et signalements pour les e-escroqueries), accessible sur masecurite.interieur.gouv.fr.

Vous n'êtes pas obligé(e) d'affronter ces démarches seul(e). L'association France Victimes propose un accompagnement gratuit aux victimes d'infractions, y compris numériques, *via* son numéro national : le 116 006. Ses juristes et psychologues peuvent vous guider dans vos démarches et vous orienter vers les structures adaptées à votre situation.

Pour en savoir plus :
cybermalveillance.gouv.fr

Arnaque amoureuse : aider sans braquer

Si l'un de vos proches est victime d'une arnaque au sentiment, évitez de le confronter directement. Maintenez le contact avec bienveillance et patience. Mais évitez de lui donner de l'argent, qui risque de finir entre les mains de l'arnaqueur. Si la situation devient préoccupante, signalez les faits aux autorités.

L'essentiel

- **Les arnaques en ligne** reposent sur de la manipulation psychologique, en jouant sur nos émotions : urgence, peur, confiance, espoir… Elles peuvent toucher tout le monde.
- **La désinformation en santé** peut avoir des conséquences délétères en retardant un diagnostic ou en détournant des patients de soins importants.
- **L'intelligence artificielle** augmente les risques avec des messages très crédibles.
- Deux réflexes sont essentiels pour limiter les risques :
  1. **Protéger** ses données.
  2. Faire preuve de la plus grande **vigilance**.