Argent facile et arnaques en réseaux

Par **Nidal Taibi**

Les publicités financières frauduleuses prolifèrent sur les réseaux sociaux. Une mécanique implacable qui mêle manipulation psychologique, appât du gain et laxisme des géants du Web.

C'est une scène ordinaire: le fil d'actualité Facebook déroule soudain «le bon plan à ne pas manquer». Un célèbre présentateur y vante une plateforme d'investissement miracle, censée transformer n'importe quel épargnant en millionnaire en quelques semaines. Le titre prometteur, «Son nouveau projet a choqué les banques!», s'accompagne d'une photo souriante de la vedette. Intrigué, l'internaute clique. Il tombe sur un article à l'allure professionnelle, imitant le site d'un grand média, où la star dévoile son «secret pour s'enrichir rapidement». Quelques liens plus loin, la page invite à investir quelques centaines d'euros pour rejoindre l'aventure.

Bienvenue dans l'arnaque financière 2.0, celle qui prolifère aujourd'hui sur les réseaux sociaux en exploitant les rêves de richesse facile. Le phénomène a pris des proportions alarmantes. Partout en Europe, les publicités frauduleuses de ce type se multiplient. En Belgique, les pertes dues à ces «arnaques à l'investissement» ont dépassé 12,5 millions d'euros sur le seul second semestre 2024, selon la FSMA, l'Autorité des services et marchés financiers. Ce chiffre ne représente que la partie émergée de l'iceberg, car nombre de victimes n'osent pas signaler l'escroquerie. Du côté du gendarme financier, la vigilance est de mise: au premier semestre 2025, la FSMA a émis huit nouvelles mises en garde, visant pas moins de 98 entités frauduleuses et 138 sites trompeurs. Plus de 65% de ces acteurs illégitimes opéraient via de fausses plateformes de trading en ligne. Comme le souligne Isabelle Marchal, assistante criminologue à l'université de Liège, les réseaux sociaux constituent désormais un environnement particulièrement propice à la diffusion de ces contenus: «Les réseaux sociaux, et plus particulièrement les plateformes Meta (Facebook, Instagram et WhatsApp), sont devenus un terrain favorable à la diffusion de publicités financières trompeuses», précise-t-elle.

DR

Avant de succomber aux sirènes d'une pub trop belle pour être vraie, un réflexe s'impose: douter.

Promesses de rendements faramineux, usurpation d'identité et technologies de pointe... Les arnaqueurs déploient des trésors d'ingéniosité pour piéger leurs proies: vidéos deepfakes d'un PDG ou d'un ministre en train de vanter une plateforme bidon, voix clonées par une intelligence artificielle imitant à la perfection votre conseiller bancaire... L'effet est généralement bluffant, et l'internaute n'y voit que du feu. Particulièrement lorsque la peur de rater «une occasion unique» entre en jeu. «Dans le cas des fausses offres publicitaires d'investissement, l'effet Fomo (*Fear of missing out*), qui renvoie à la peur de rater "le train d'une affaire en or", une opportunité unique de se faire de l'argent, est largement exploité, développe Isabelle Marchal. Cet effet permet d'expliquer, entre autres, pourquoi certains individus tombent dans le piège de ces publicités. Attirés par l'aubaine de gains importants, rapides et faciles, ils cèdent à l'avidité, un appel au profit, d'autant plus "pressant" que l'offre est présentée comme limitée dans le temps.» En exploitant cette impulsion presque primitive, les fraudeurs parviennent ainsi à court-circuiter toute forme de prudence ou de réflexion critique.

Les rouages psychologiques d'une fraude bien huilée

Derrière ces stratagèmes numériques se cache une mécanique bien rodée où se mêlent psychologie et technologie. «Ces publicités, qui font miroiter la possibilité d'obtenir des investissements ou des conseils d'investissement "exclusifs" et prétendument très lucratifs existent depuis un certain temps, mais sont désormais à la fois facilitées et potentiellement plus efficaces en raison de l'utilisation d'outils d'intelligence artificielle générative, poursuit la criminologue. Aussi, la confiance inspirée par des visages connus et souvent choisis, parce que synonymes de sérieux ou d'intelligence, apparaît centrale dans la mécanique criminelle.» En d'autres termes, les escrocs exploitent non ...

… seulement les failles des algorithmes, mais aussi celles de la perception humaine, la crédulité suscitée par des visages familiers devenant une arme redoutable.

Les escrocs actionnent à la fois des leviers techniques et psychologiques, brouillant la frontière entre le vrai et le faux. D'un côté, ils misent sur la haute technologie: base de données volées, usurpation d'identité numérique, messages calibrés par des algorithmes. De l'autre, ils exploitent les failles émotionnelles: cupidité, confiance en l'autorité et, surtout, impulsivité. Lorsque tout semble crédible, l'internaute a tendance à baisser la garde. Ainsi, les fraudeurs parviennent à instaurer un climat de confiance factice (par exemple, en appelant depuis un faux numéro de la banque) tout en semant la panique pour précipiter la décision: «Vous risquez de tout perdre si vous n'agissez pas vite!». Ce mélange d'ingénierie sociale et de technologie avancée fait des ravages.

Longtemps, on a cru que seules les personnes âgées ou naïves se faisaient avoir. La réalité, c'est que personne n'est épargné. Les cyberescrocs adaptent d'ailleurs leur discours à leur cible: vaines promesses de rente viagère pour les seniors, mirage du jackpot crypto pour les trentenaires en quête d'indépendance financière… Résultat: la génération ultraconnectée se fait elle-même piéger.

Les plateformes visées

Cette épidémie d'arnaques pose frontalement la question des responsabilités des plateformes qui les hébergent. Meta (maison mère de Facebook, Instagram et WhatsApp) est particulièrement dans le viseur. En Europe, autorités et experts ont multiplié mises en demeure et rapports pour pousser le géant à agir, face à la prolifération de scams dopés aux deepfakes et aux fausses publicités trompeuses. Officiellement, Meta assure investir dans des filtres automatisés et de la modération humaine pour bloquer ces contenus illicites. Mais sur le terrain, le compte n'y est pas. Un audit interne soulignait en 2024 que le groupe ne disposait que de 5.548 modérateurs pour l'ensemble des 24 langues officielles de l'UE. Un chiffre dérisoire au vu des 260 millions d'utilisateurs européens actifs chaque mois. Des observateurs du secteur soulignent que la quête du volume, au cœur du modèle publicitaire de la firme, s'est longtemps accompagnée d'un certain laxisme dans le contrôle de ces publicités trompeuses. D'après *The Wall Street Journal*, malgré la hausse inquiétante des scams en ligne, Meta hésiterait à serrer la vis aux annonceurs douteux qui contribuent à ses 160 milliards de dollars de revenus publicitaires annuels. Pendant des années, les arnaqueurs ont donc pu acheter des espaces publicitaires comme les autres et diffuser leurs pièges à grande échelle sans entraves.

«L'effet Fomo, qui renvoie à la peur de rater une opportunité unique de se faire de l'argent, est largement exploité.»

La législation tente aussi de rattraper son retard. Entré en vigueur en 2023, le Digital Services Act (DSA) européen impose désormais aux géants du Web un devoir de vigilance accru: identification rigoureuse des annonceurs, suppression rapide des contenus illicites (dont les arnaques financières), transparence sur les algorithmes, audits externes. Les manquements pourront valoir aux plateformes récalcitrantes des amendes salées. Dans le même esprit, les régulateurs internationaux appellent à la mobilisation générale: en mai 2025, l'Iosco (Organisation mondiale des autorités des marchés financiers) a exhorté moteurs de recherche, réseaux sociaux et messageries à rejoindre le combat contre ces acteurs illégitimes en ligne.

Sur le terrain, la riposte s'organise. En Belgique, la FSMA alimente constamment une liste noire des sites ainsi que des intermédiaires douteux, et multiplie les campagnes de sensibilisation. La police et les médias relaient le message. Ainsi, en octobre 2025, la VRT a lancé une campagne choc intitulée «In het echt zou je het niet geloven, waarom dan wel online?» (Dans la vraie vie, vous n'y croiriez pas. Pourquoi le faire en ligne?). Ce spot met en scène des célébrités flamandes dans des situations volontairement absurdes, impossibles à croire dans la réalité, afin d'éveiller l'esprit critique des internautes face aux promesses irréelles. L'objectif est de rappeler à chacun que les arnaques prospèrent sur la crédulité et que, pour ne plus en être victime, il faut apprendre à repérer les signaux d'alerte (offres trop alléchantes, urgence suspecte, sources inconnues, etc.) avant de cliquer.

Les autorités peuvent bien multiplier les garde-fous et les campagnes d'information, la vigilance individuelle demeure néanmoins l'arme la plus efficace. Avant de succomber aux sirènes d'une publicité trop belle pour être vraie, un réflexe s'impose: douter. Car en matière d'investissement, les miracles n'existent pas, et personne ne s'enrichira en quelques clics sur la recommandation d'un inconnu sur Facebook. ●