FRAUDES ET ARNAQUES FINANCIÈRES EN LIGNE À L'ÈRE DE L'INTELLIGENCE ARTICIFIELLE

RESTEZ VIGILANT ET PROTÉGEZ-VOUS

Les fraudes et arnaques financières en ligne ne sont pas nouvelles, mais l'intelligence artificielle (IA) les rend toujours plus convaincantes et difficiles à repérer. Les escrocs n'utilisent maintenant plus seulement de faux messages et sites internet ou de faux profils de célébrités. Ils peuvent également, grâce à l'IA, produire des audios ou des vidéos dont les protagonistes ressemblent à votre banquier, à vos amis ou à des membres de votre famille pour vous tromper.

Ils peuvent alors vous contacter via les réseaux sociaux, des e-mails, le téléphone ou des applications de messagerie avec des textes, des images et des voix qui semblent bien réels.

Trompés par ces leurres, vous pouvez être victime d'un vol de vos données personnelles ou de pertes financières. Soyez donc prudent et suivez ces conseils clés pour vous protéger :

Restez vigilant face aux fraudes et arnaques financières en ligne qui peuvent être améliorées grâce à l'IA, par exemple, l'usurpation d'identité, le hameçonnage (*phishing*), les arnaques à l'investissement et à l'assurance, voire même les fraudes et arnaques aux sentiments. Pour en savoir plus sur les différents types de fraudes et d'arnaques voir pages 5 à 7.

Et pour les fraudes et arnaques spécifiques aux crypto-actifs voir ( ).

Soyez attentifs aux signaux d'alerte : apprenez à reconnaître les comportements, messages ou offres suspects (voir page 2);

Protégez-vous : sécurisez vos équipements et vos informations personnelles (voir page 3);

Sachez quoi faire si vous êtes victime d'une fraude ou d'une arnaque (voir page 4).

Les signaux d'alerte

Une promesse trop belle pour être vraie.

Un appel inattendu provenant d'un numéro inconnu.

Une demande urgente d'argent ou de renseignements personnels, y compris de la part d'une personne prétendant être un membre de la famille, un ami ou même une personnalité publique.

Une demande d'accepter la prise de contrôle à distance de votre appareil, de télécharger une application, de scanner un QR code ou de cliquer sur un lien.

Une demande d'informations personnelles ou de détails bancaires (par exemple, mots de passe, numéros de carte de crédit, identifiants bancaires sur Internet ou codes de sécurité).

Une demande de paiement via des moyens de paiement non traçables (par exemple, crypto-actifs, cartes-cadeaux, virements bancaires ou cartes de débit prépayées).

Une adresse e-mail ou un lien suspect ou incorrect (par exemple, des erreurs d'orthographe dans l'URL ou des adresses Internet inhabituelles).

Une pièce jointe provenant d'une source inconnue, en particulier des fichiers portant les extensions .exe, .scr, .zip ou un des fichiers Office pouvant contenir des macros (.docm, .xlsm).

Une grammaire incorrecte ou une mise en forme douteuse dans un document d'apparence officielle, même si des outils d'IA permettent aujourd'hui aux fraudeurs de masquer ces défauts plus efficacement.

Un site Internet qui a l'air professionnel mais qui manque de coordonnées vérifiées ou d'informations d'immatriculation de l'entreprise.

Une intonation de votre interlocuteur qui ne semble pas naturelle, manque de pauses ou semble trop fluide ou robotique. Il peut s'agir de clonage vocal, même si, là encore, les IA permettent de générer des voix de plus en plus naturelles.

Des vidéos où la voix peut sembler robotique ou trop lisse, les mouvements des lèvres et les expressions faciales sont mal alignés avec la parole ou l'arrière-plan, l'éclairage et les ombres peuvent être incohérents. Ce sont souvent des vidéos générées par l'IA, dites « *deepfakes* ».

Précautions pour vous protéger

1 **Ne partagez jamais d'informations personnelles ou bancaires :**

Les entreprises légitimes ne vous demanderont jamais vos codes PIN, mots de passe, identifiants bancaires ou codes de sécurité par e-mail, SMS, réseaux sociaux ou téléphone.

2 **Faites une pause et réfléchissez avant d'agir :**

Ne vous précipitez pas pour envoyer de l'argent, partager des informations ou cliquer sur des liens : les escrocs créent délibérément un sentiment d'urgence (par exemple, prétendus problèmes informatiques avec votre banque, appels d'urgence impliquant vos amis et les membres de votre famille, langage menaçant, etc.). Au moindre doute, mettez fin à l'appel et vérifiez soigneusement la source ou l'identité de la personne qui vous contacte.

3 **Vérifiez attentivement la source et l'identité des contacts :**

- Vérifiez toujours d'où proviennent les SMS, les appels, les e-mails et les liens- même s'ils semblent officiels, ou paraissent provenir d'un ami, d'un membre de votre famille, ou d'une personnalité publique. Lorsque vous appelez ou envoyez un SMS à votre famille ou à vos amis, utilisez toujours un numéro connu ou trouvé via un canal de confiance. Soyez attentifs aux fautes d'orthographe, aux URL étranges ou aux indicateurs de sécurité manquants (par exemple, vérifiez que le lien vers le site internet inclut un « s » dans « HTTPS ». Vérifiez qu'aucune lettre n'a été ajoutée ou est manquante dans le nom de l'entreprise figurant dans l'URL.

- N'ouvrez pas de liens contenus dans des messages non sollicités, n'installez que des applications officielles via des boutiques d'applications de confiance et ne scannez pas de QR codes inconnus.

- Convenez avec votre famille d'un « mot de sécurité » : une phrase secrète par exemple que vous pouvez utiliser pour confirmer l'identité de votre interlocuteur si quelqu'un avec une voix familière vous appelle avec une demande urgente d'argent.

- Utilisez les coordonnées vérifiées pour contacter directement les entreprises ou les personnes et ne vous fiez jamais aux coordonnées contenues dans un message suspect. Recherchez le nom de l'entreprise de manière indépendante, utilisez des annuaires commerciaux vérifiés, ou utilisez des coordonnées de contact précédemment confirmées. Les escrocs peuvent prétendre être autorisés à exercer une activité financière ou imiter le site Internet d'une société autorisée à exercer cette activité. Vérifiez si des alertes ont été émises par votre autorité financière nationale (↖) ou figurent dans la liste I-SCAN de l'OICV (iosco.org/i-scan/). Pour les fournisseurs de crypto-actifs, vérifiez s'ils sont agréés pour exercer dans l'UE, par exemple, en consultant le registre de l'ESMA (↖).

4 **Faites attention aux techniques d'escroquerie potentiellement améliorées par l'IA :**

À mesure que l'IA progresse, les arnaques deviennent plus convaincantes et plus difficiles à détecter, même en ayant en tête les meilleurs conseils de sécurité. Si quelque chose vous semble inhabituel ou si vous détectez l'un des signaux d'alerte décrits ci-dessus, arrêtez-vous et examinez attentivement toutes les informations dont vous disposez.

5 **N'installez jamais de logiciel d'accès à distance ou ne partagez jamais votre écran si vous n'êtes pas sûr de la légitimité de la demande :**

Par exemple, les banques et les institutions financières ne vous le demanderont jamais.

6 **Sécuriser vos appareils et vos comptes :**

Utilisez des mots de passe robustes et uniques, gardez-les secrets et ne réutilisez pas les mêmes informations d'identification/authentification sur différentes plateformes. Activez l'authentification forte lorsqu'elle est disponible. Vous trouverez quelques conseils sur la création de vos mots de passe ici (↖). Gardez tous vos logiciels à jour et activez votre protection antivirus.

7 **Soyez prudent face aux opportunités d'investissement non sollicitées et limitées dans le temps :**

Si cela semble trop beau pour être vrai, c'est probablement une arnaque.

8 **Réfléchissez avant de partager des informations sur les réseaux sociaux :**

Les informations et les photos que vous postez sur les groupes de discussion, les forums, et réseaux sociaux en général peuvent être précieuses pour les escrocs. Révéler trop de choses sur vous-même ou sur vos investissements peut faire de vous une cible plus facile.

Que faire si vous êtes victime d'une fraude ou d'une arnaque

Arrêtez immédiatement les transactions avec le fraudeur :

Bloquez tout autre transfert d'argent vers des comptes suspects pour éviter des pertes supplémentaires. Arrêtez tout contact avec les escrocs – ignorez leurs appels et leurs emails et, si possible, bloquez les contacts téléphoniques et les expéditeurs de messages.

Contactez votre banque ou établissement financier :

Informez immédiatement votre banque ou votre établissement financier via les canaux de contact officiels, afin d'étudier les options de gel ou d'inversion des transactions encore en cours.

Modifiez vos mots de passe sur tous vos appareils, applications et sites internet :

Les escrocs achètent des mots de passe divulgués en ligne et tentent de les utiliser sur tous les comptes où vous auriez pu vous identifier avec votre adresse courriel. Changer un seul mot de passe ne suffit pas : assurez-vous de tous les changer, afin que les escrocs ne puissent pas les réutiliser.

Signalez et alertez :

Signalez l'incident à la police ou à votre autorité financière nationale (↖) et informez vos proches afin de participer à la sensibilisation du public. Ces actions peuvent vous aider à vous protéger et contribuent à protéger les autres.

Méfiez-vous de l'arnaque au recouvrement de fonds :

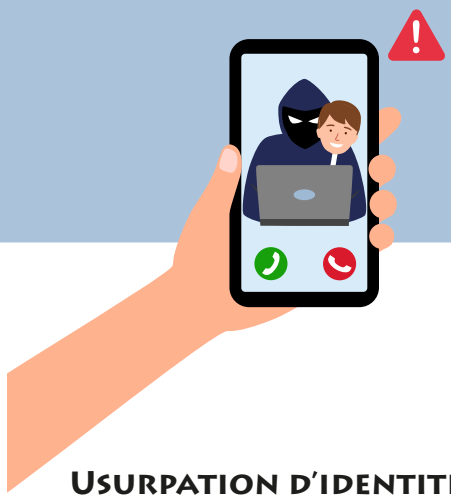
Dans cette fraude, un escroc vous contacte en sachant que vous avez été victime d'une arnaque antérieure. Cette personne prétend représenter une autorité publique (par exemple, la police, une autorité fiscale ou financière, etc.) et offre de récupérer votre argent perdu, moyennant bien sûr des frais. C'est une tentative de vous arnaquer une nouvelle fois. Rappelez-vous : être arnaqué une fois ne vous empêche pas d'être arnaqué à nouveau.

Autorité bancaire européenne, Autorité européenne des assurances et des pensions professionnelles, Autorité européenne des marchés financiers, 2025

Luxembourg: Office des publications de l'Union européenne, 2025

PDF ISBN 978-92-9407-244-3 doi:10.2853/5514216 DZ-01-25-132-FR-N

TYPES DE FRAUDES ET D'ARNAQUES FINANCIÈRES EN LIGNE GÉNÉRÉES PAR L'IA



Usurpation d'identité et utilisation de *deepfakes*

Vous recevez un appel inattendu d'une personne prétendant travailler dans votre banque, une autorité publique (par exemple, la police, les impôts ou une autorité financière, etc.), un distributeur d'assurances ou une société informatique. Votre interlocuteur peut vous inciter à transférer des fonds pour les garder en sécurité, prétextant une activité suspecte sur votre compte ou un problème avec votre contrat d'assurance. Il peut vous demander de divulguer vos coordonnées bancaires (par exemple, un numéro de carte de paiement, des identifiants bancaires en ligne ou des mots de passe), de cliquer sur un lien ou d'installer un logiciel, en prétendant qu'il pourra ainsi résoudre rapidement le soi-disant problème. L'appelant peut utiliser un numéro falsifié, correspondant par exemple au numéro de téléphone de votre banque pour paraître légitime (usurpation d'identité).

Pour mieux vous convaincre, les escrocs peuvent utiliser l'IA pour créer des « deepfakes » : il s'agit de fausses vidéos, images ou sons qui imitent la voix d'une personne (par exemple, votre banquier ou un membre de votre famille), son visage (par exemple, une célébrité) ou ses mouvements. **C'est le « deepfake ».**

Ce qui pourrait arriver :

En créant un sentiment d'urgence, l'escroc vous manipule et vous amène à réaliser des actions que vous n'aviez pas l'intention de faire, telles qu'envoyer de l'argent sur son compte, cliquer sur un lien malveillant ou installer un logiciel malveillant sur votre appareil. Ces actions peuvent permettre à l'escroc d'accéder à vos informations bancaires avec lesquelles il pourra changer votre mot de passe, accéder à votre compte bancaire et voler votre argent. Rappelez-vous : le simple fait que votre interlocuteur connaisse des informations personnelles vous concernant ne signifie pas qu'il est digne de confiance.

Hameçonnage (*phishing*) et ingénierie sociale

Vous recevez un e-mail ou un SMS qui semble provenir de votre banque ou d'un établissement financier, vous avertissant d'une « activité suspecte » sur votre compte. Le logo, la mise en page et la rédaction du texte semblent professionnels, et le message peut apparaître dans le fil de conversation avec votre banque. Le message vous invite à cliquer sur un lien pour vérifier votre compte ou réinitialiser votre mot de passe. Ce lien mène à un faux site Internet qui semble identique à celui de votre banque en ligne et vous demande vos informations de connexion. Vous saisissez ces informations et, sans vous en rendre compte, vous venez de les fournir à un escroc.

Les escrocs utilisent l'IA pour créer des messages de *phishing* convaincants en analysant les données des réseaux sociaux concernant leurs victimes et en adaptant, grâce à ces données, le contenu du message à chaque cible.

Ce qui pourrait arriver :

L'escroc accède à votre compte bancaire et vole votre argent ou crée un compte à votre nom grâce à vos données personnelles pour commettre une fraude.

Arnaque à l'investissement ou à l'assurance

Vous voyez une publicité sur les réseaux sociaux ou un site internet faisant la promotion d'une soi-disant « offre d'investissement à durée limitée à fort rendement et faible risque » ou d'une « remise à durée limitée » sur une assurance de la part d'une entreprise bien connue. L'annonce présente une photo d'une célébrité et des incitations fortes à profiter de l'opportunité présentée. Après avoir exprimé votre intérêt en cliquant sur un lien ou en remplissant un formulaire, vous êtes contacté et redirigé vers une plateforme ou un canal de messagerie où vous recevez des conseils et des documents qui vous paraissent professionnels. Vous êtes encouragé à investir un petit montant, suivi souvent de sommes plus importantes, et on vous convainc de transférer l'argent vers ce qui semble être un compte sécurisé.

Les fraudeurs utilisent des outils d'IA pour rendre ces fausses propositions très convaincantes et difficiles à détecter. Ils utilisent également des robots alimentés par l'IA pour créer de faux comptes qui interagissent avec vous sur les réseaux sociaux, diffusent de la désinformation et simulent des comportements réels pour gagner votre confiance et influencer vos décisions.

Ce qui pourrait arriver :

Alors que vous essayez de retirer votre argent ou de faire une réclamation, votre contact est injoignable. Vous découvrez que l'entreprise n'existe pas ou que le risque pour lequel vous avez payé une assurance n'est pas couvert. Vous réalisez alors que vous avez envoyé de l'argent à un escroc. Malheureusement, vous ne pouvez généralement pas récupérer cet argent et vos données personnelles et financières peuvent être utilisées pour commettre d'autres arnaques (par exemple, signer des contrats en votre nom qui pourraient vous conduire à perdre encore plus d'argent).

Arnaque aux sentiments

Vous avez été contacté sur les réseaux sociaux, via une application de rencontres, ou par téléphone / message par quelqu'un que vous n'avez jamais rencontré dans la vie réelle. Cette personne s'engage dans des conversations fréquentes, personnelles et romantiques avec vous, construisant ainsi une relation de confiance. Au fil du temps, le thème de la conversation se déplace vers des sujets d'argent ou d'opportunités financières, tels que les investissements en crypto-actifs avec des promesses de rendements élevés, minorant les risques. La personne vous demande de transférer de l'argent sur un compte ou vous guide à travers la création d'un compte. Souvent, elle vous demande un petit dépôt initial qui sera effectivement rémunéré pour donner une apparence légitime à l'opération avant de vous encourager à investir davantage.

Les fraudeurs utilisent l'IA pour générer de faux profils, identifier leurs victimes sur les réseaux sociaux ou les applications de rencontres à l'aide des données que vous avez mises à disposition, ou utilisent des *chatbots* pour générer les messages qu'ils vous envoient.

Ce qui pourrait arriver :

L'escroc vous fait verser autant d'argent que possible, puis coupe toute communication avec vous et disparaît. Outre la perte financière, les informations personnelles que vous avez partagées peuvent être utilisées pour cibler vos amis et votre famille ou pour une future usurpation d'identité qui pourra avoir de lourdes conséquences financières et juridiques pour vous (par exemple, le fraudeur pourrait effectuer des achats, contracter des prêts en votre nom, ou vous pourriez être tenu responsable de dettes ou de délits commis sous votre nom jusqu'à preuve du contraire).

Arnaque à l'achat

Vous remarquez une offre attrayante sur une *marketplace* (plateforme de vente en ligne) en ligne. La société proposant le produit demande un paiement en dehors de la plateforme officielle, affirmant qu'elle utilise un « système de paiement sécurisé », plus avantageux pour vous, et vous envoie un lien pour finaliser l'achat. Le lien vous redirige vers une page d'authentification bancaire frauduleuse qui imite le site officiel de la banque, de sorte que vous entrez vos coordonnées bancaires en toute confiance pour effectuer le paiement.

Les escrocs utilisent l'IA pour créer de faux sites internet bancaires très convaincants, des fausses confirmations de commandes et factures. L'IA les aide à imiter le ton, l'image de marque et le style de vraies entreprises. Dans certains cas, ils utilisent des *chatbots* pour répondre aux questions et rendre l'affaire plus crédible.

Ce qui pourrait arriver :

Le paiement via un lien tiers contourne les protections de la marketplace (plateforme de vente en ligne). L'escroc obtient vos informations de connexion à votre compte bancaire, s'y connecte et vole votre argent.