FRAUDES FINANCIÈRES ET ESCROQUERIES EN LIGNE À L'ÈRE DE L'INTELLIGENCE ARTIFICIELLE

RESTEZ VIGILANT(E) ET PROTÉGEZ-VOUS

Les fraudes et escroqueries financières en ligne ne sont pas nouvelles, mais l'intelligence artificielle (IA) les a rendues plus sophistiquées et plus difficiles à repérer. Les criminels utilisent maintenant de faux messages et sites Internet, de faux profils de célébrités et même des voix ou des vidéos générées par l'IA qui peuvent imiter votre banquier, vos amis ou votre famille pour vous leurrer.

Ils vous contactent souvent via les réseaux sociaux, des applications de messagerie, des courriels ou des appels inattendus qui ont l'air réelles.

Vous pouvez faire face à des risques tels que la perte financière, l'usurpation d'identité et la détresse émotionnelle. Soyez prudent(e) et suivez ces conseils clés pour rester en sécurité :

Restez attentif(ve) aux fraudes et aux escroqueries financières en ligne générées par l'IA :
Par exemple, l'usurpation d'identité, le *phishing* (hameçonnage), les escroqueries à l'investissement et à l'assurance, et même les fraudes et escroqueries sentimentales. Pour en savoir plus sur les différents types de fraudes et d'escroqueries (voir pages 5, 6 et 7).

Et pour les fraudes et escroqueries spécifiques aux crypto-actifs veuillez consulter la fiche d'information sur les fraudes et escroqueries liées aux crypto-actifs ( ).

Repérez les signes d'alerte :
Apprenez à reconnaître les comportements, messages ou offres suspects (voir page 2) ;

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

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

Signaux d'alerte

Une promesse qui semble 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 pour prendre le contrôle de votre appareil à distance, télécharger une application, scanner un QR code ou cliquer sur un lien

Une demande d'informations personnelles ou de coordonnées 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 méthodes intraçables (par exemple crypto-actifs, cartes-cadeaux, virements bancaires ou cartes de débit prépayées)

Une adresse courriel ou un lien suspect(e) ou incorrect(e) (par exemple, des fautes d'orthographe dans l'URL ou des adresses Internet inhabituelles)

Une pièce jointe provenant d'une source inconnue, en particulier les fichiers Office .exe, .scr, .zip ou avec macros (.docm, .xlsm)

Une grammaire ou mise en forme approximative dans un document d'apparence officielle, bien que l'IA permette aux fraudeurs de masquer ces failles plus efficacement

Un site Internet qui a l'air professionnel mais sans coordonnées vérifiées ni informations sur l'enregistrement de l'entreprise

Une intonation qui ne semble pas naturelle, qui manque de pauses et semble trop fluide ou robotique. Faites attention au « clonage vocal », bien que la voix générée par l'IA puisse également sembler très naturelle

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

Étapes 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 en ligne ou codes de sécurité par courriel, SMS, réseaux sociaux ou téléphone.

2 **Prenez un moment pour réfléchir avant d'agir :**

Ne vous précipitez jamais pour envoyer de l'argent, partager des informations ou cliquer sur des liens. Les escrocs créent délibérément un sentiment d'urgence (par exemple, problèmes informatiques avec votre banque, appels d'urgence impliquant vos amis et des membres de votre famille, langage menaçant, etc.). Si vous avez le moindre doute, n'agissez pas, raccrochez et vérifiez soigneusement la source ou l'identité.

3 **Vérifiez attentivement la source/l'identité :**

- Vérifiez toujours d'où proviennent les messages, les appels, les courriels et les liens- même s'ils semblent officiels, semblent provenir d'un proche, ou même d'une personnalité publique. Par exemple, appelez ou envoyez un SMS à votre famille et à vos amis en utilisant un numéro connu via un canal de confiance ; recherchez des fautes d'orthographe, des URL étranges ou des indicateurs de sécurité manquants (par exemple, vérifier que le lien du site Internet inclut un « s » dans « HTTPS » pour vous assurer que le site Internet est sécurisé, et vérifiez toute lettre ajoutée ou manquante dans le nom de l'entreprise).

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

- Convenez avec votre famille d'un « mot de sécurité » : une phrase secrète que vous pouvez utiliser pour confirmer l'identité d'un proche si quelqu'un avec une voix familière vous appelle et vous demande de l'argent de toute urgence en prétendant être un membre de la famille (par exemple, parents, sœur / frère, enfant).

- Utilisez des coordonnées vérifiées pour contacter directement une entreprise ou un individu et ne vous fiez jamais aux coordonnées fournies par le fraudeur présumé (par exemple, recherchez vous-même le nom de l'entreprise, utilisez des annuaires commerciaux vérifiés, des méthodes de contact précédemment confirmées). Certains escrocs peuvent prétendre être autorisés ou imiter le site Internet d'une société autorisée. Vérifiez si des avertissements ont été émis par votre autorité financière nationale ou inclus dans la liste I-SCAN de l'OICV (iosco.org/i-scan/). Pour les fournisseurs de cryptomonnaies, vérifiez s'ils sont autorisés dans l'UE (par exemple, vérifiez le registre de l'ESMA ( ).

4 **Faites attention aux potentielles manipulations via l'IA :**

À mesure que la technologie de l'IA progresse, les escroqueries deviennent plus convaincantes que jamais - même avec les meilleurs conseils de sécurité. Si quelque chose vous semble inhabituel ou si vous détectez l'un des signes avant-coureurs décrits ci-dessus, arrêtez-vous et réévaluez la situation.

5 **N'installez jamais de logiciel d'accès à distance ou ne partagez jamais votre écran :**

Les banques et les institutions financières ne vous le demanderont jamais.

6 **Sécurisez vos appareils et vos comptes :**

Utilisez des mots de passe forts et uniques, gardez-les secrets et évitez d'utiliser les mêmes informations d'identification sur différentes plates-formes. Activez l'authentification multifacteur dans la mesure du possible. Vous pouvez obtenir quelques conseils sur les mots de passe sous . Gardez vos logiciels et votre protection antivirus à jour et activés.

7 **Soyez prudent(e) avec les opportunités d'investissement inattendues et limitées dans le temps :**

Si cela semble trop beau pour être vrai, c'est probablement le cas.

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

Les groupes de discussion, les forums, les publications sur les réseaux sociaux et les photos peuvent être des sources d'informations précieuses pour les fraudeurs. Révéler trop de choses sur vous ou sur vos investissements peut faire de vous une cible facile.

Que faire lorsque vous êtes victime d'une fraude ou d'une escroquerie

Arrêtez immédiatement les transactions :

Bloquez toute nouvelle opération vers des comptes suspects afin d'éviter des pertes supplémentaires. Cessez tout contact avec les escrocs : ignorez leurs appels et leurs courriels et bloquez l'expéditeur.

Contactez votre banque ou société financière :

Informez-les immédiatement via les canaux de contact officiels afin de voir les possibilités de geler ou d'inverser les transactions.

Modifiez vos mots de passe sur tous vos appareils et applications/sites Internet :

Les fraudeurs achètent des mots de passe divulgués en ligne et les essaient sur plusieurs comptes. Changer un seul mot de passe ne suffit pas : changez-les tous afin que les fraudeurs ne puissent pas les réutiliser.

Signalez l'incident et alertez votre entourage :

Signalez l'incident à la police et, si pertinent, à la CSSF (https://www.cssf.lu/) et informez votre entourage (par exemple, vos amis et votre famille) afin de sensibiliser le public. Ces actions peuvent vous aider à vous protéger et à protéger les autres.

Méfiez-vous de la fraude de type « *recovery room* » :

Le fraudeur peut vous contacter en sachant que vous avez déjà été victime d'une escroquerie, prétendant être une autorité publique (par exemple, la police, l'autorité fiscale ou financière, etc.) et vous proposant de récupérer votre argent perdu moyennant des frais. C'est souvent une nouvelle tentative de vous arnaquer. Rappelez-vous : le fait d'avoir été victime d'une arnaque une fois ne vous empêche pas d'être victime d'une nouvelle arnaque.

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'EXCROQUERIES FINANCIÈRES EN LIGNE GÉNÉRÉES PAR L'IA

Escroquerie par usurpation d'identité et utilisation de *deepfakes*

Vous recevez un appel inattendu d'une personne prétendant être votre banque, une autorité publique (par exemple, la police, l'autorité fiscale ou financière, etc.), une compagnie d'assurances, une société informatique ou même un membre de votre famille. L'interlocuteur peut vous exhorter à transférer des fonds « pour les garder en sécurité », évoquant une activité suspecte sur votre compte ou votre police d'assurance. Il ou elle peut également vous demander de divulguer vos coordonnées bancaires (par exemple, numéro de carte de paiement, identifiants bancaires en ligne ou mots de passe), de cliquer sur un lien ou d'installer un logiciel, en prétendant qu'il peut résoudre rapidement le problème. L'interlocuteur peut utiliser un numéro falsifié, correspondant souvent au numéro de téléphone de votre banque pour paraître légitime (*spoofing*).

Les escrocs peuvent utiliser l'IA pour créer de fausses vidéos, images ou audios qui imitent la voix d'une personne (par exemple, votre banquier ou un membre de votre famille), son visage (par exemple, d'une célébrité) ou ses mouvements. **Cette pratique est connue sous le nom de « *deepfake* ».**

Ce qui pourrait arriver :

En mentionnant des données personnelles et en créant un sentiment d'urgence, l'escroc vous pousse à agir sans réfléchir, par exemple, à envoyer de l'argent, à cliquer sur un lien malveillant ou à installer un logiciel malveillant sur votre appareil. Cela peut donner à l'escroc un accès direct à vos informations d'identification bancaires. Avec ces informations, il ou elle peut changer votre mot de passe, accéder à votre compte bancaire et voler votre argent. Rappelez-vous : le simple fait qu'un interlocuteur connaisse des informations personnelles vous concernant ne signifie pas qu'il est digne de confiance.

Hameçonnage (*phishing*) et ingénierie sociale

Vous recevez un courriel ou un message qui semble provenir de votre banque ou d'une société financière, vous alertant d'une « activité suspecte » sur votre compte. Le logo, la mise en page et le style semblent professionnels, et le message peut apparaître dans le même fil de discussion que d'autres conversations avec votre banque. Le message vous invite à cliquer sur un lien pour vérifier votre compte ou réinitialiser votre mot de passe. Le lien mène à un faux site Internet qui semble identique à celui de votre banque en ligne. Sans vous en rendre compte, vous saisissez vos coordonnées sur un site Internet conçu pour voler vos informations personnelles.

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

Ce qui pourrait arriver :

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

Escroquerie à l'investissement ou à l'assurance

Vous voyez une publicité sur les réseaux sociaux ou un site Internet faisant la promotion d'une « opportunité d'investissement à durée limitée à faible risque » ou d'une « remise à durée limitée » sur une assurance d'une entreprise prétendument réputée. L'annonce présente une photo d'une célébrité et des recommandations qui sont souvent fausses. Après avoir exprimé votre intérêt en cliquant sur un lien ou en remplissant un formulaire, vous êtes contacté(e) et redirigé(e) vers une plateforme ou un canal de messagerie où vous recevez des conseils et des documents d'aspect professionnel. Vous êtes encouragé(e) à investir un petit montant, suivi de sommes plus importantes, ou à payer une prime dans ce qui semble être un compte sécurisé.

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

Ce qui pourrait arriver :

Après avoir essayé de retirer votre argent ou de faire une réclamation, le contact cesse de répondre. Vous découvrez que l'entreprise n'existe pas ou que le risque que vous aviez assuré n'est pas couvert. Vous réalisez alors que vous avez envoyé de l'argent directement à un escroc dans le cadre d'un stratagème frauduleux. Malheureusement, vous ne pouvez pas récupérer votre argent et vos données personnelles et financières peuvent être utilisées pour commettre d'autres fraudes (par exemple, signer des contrats en votre nom, ce qui pourrait vous conduire à perdre encore plus d'argent).

Fraude et escroquerie sentimentale

Vous avez été contacté sur les réseaux sociaux, des applications de rencontre, ou par téléphone/SMS par quelqu'un que vous n'avez jamais rencontré dans la vie réelle. Cette personne s'engage dans des conversations fréquentes, personnelles et romantiques, instaurant un climat de confiance en utilisant de faux profils. Au fil du temps, la conversation s'oriente vers l'argent ou les opportunités financières, telles que des investissements dans des crypto-actifs avec la promesse de rendements élevés et de faibles risques. La personne vous demande de transférer de l'argent sur un compte ou vous guide pour créer un compte et faire un petit dépôt initial afin de rendre le système crédible 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 rencontre à partir des données que vous avez mises à disposition, ou utilisent des chatbots pour envoyer des messages.

Ce qui pourrait arriver :

L'escroc extorque autant d'argent que possible, puis coupe toute communication et disparaît. Le site Internet ou l'application d'investissement frauduleux est mis hors ligne, ce qui vous empêche d'accéder aux prétendus investissements. Outre la perte financière, les informations personnelles que vous avez partagées pourraient être utilisées pour cibler vos proches ou pour usurper votre identité, ce qui peut avoir des conséquences financières ou juridiques (par exemple, le fraudeur pourrait effectuer des achats, contracter des prêts en votre nom, ou vous pourriez être tenu responsable de dettes ou de crimes commis sous votre nom jusqu'à preuve du contraire).

Escroquerie à l'achat

Vous tombez sur une offre attrayante pour un achat sur un marché en ligne. La société proposant la bonne affaire vous demande de payer en dehors de la plateforme officielle, affirmant utiliser un « système de paiement sécurisé », 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 et utilise son logo et sa mise en page. Vous saisissez vos coordonnées bancaires en ligne pour effectuer le paiement.

Les escrocs utilisent l'IA pour créer de faux sites Internet bancaires très crédibles, de fausses confirmations de commande et de fausses 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 IA pour répondre aux questions et rendre l'offre plus crédible.

Ce qui pourrait arriver :

Le paiement via un lien tiers contourne les protections de la place de marché. L'escroc obtient vos informations de connexion et accède à votre compte bancaire, ce qui lui permet de voler votre argent.