FRAUDES FINANCIÈRES EN LIGNE ET SCAMS DANS UN MONDE AVEC L'INTELLIGENCE ARTIFICIELLE

RESTEZ VIGILANT ET PROTÉGEZ-VOUS

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

Ils vous contactent souvent via les réseaux sociaux, des e-mails, des appels inattendus et des applications de messagerie qui semblent réelles.

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

Restez attentif aux fraudes et arnaques financières en ligne qui peuvent être améliorée 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-actif 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); et

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

Signaux d'avertissement

Une promesse qui semble trop belle pour être vraie.

Un appel inattendu 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, télécharger une application, scanner un code QR ou 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 méthodes non-traçables (par exemple les cryptos, les cartes-cadeaux, des services de paiement instantané des cartes de débit prépayées).

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

Une pièce jointe provenant d'une source inconnue, en particulier au format .exe, .scr, .zip ou un fichier Office compatible macro (.docm, .xlsm).

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

Un site Web qui a l'air professionnel mais où il manque les coordonnées ou les informations légales de l'entreprise.

Une intonation qui ne semble pas naturelle, un propos qui manque de pauses et semble trop fluide ou robotique. Soyez attentifs au clonage vocal, ainsi qu'à la parole générée par l'IA qui peut également sembler très naturelle.

Les vidéos où les voix peuvent sembler robotiques ou trop lisses, où les mouvements des lèvres et les expressions faciales peuvent être mal alignés avec la parole, et où, à l'arrière-plan, l'éclairage et les ombres apparaissent incohérents. Il s'agira souvent de 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 sur Internet ou codes de sécurité par e-mail, messages, médias 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 Internet: les escrocs créent délibérément un sentiment d'urgence (par exemple, en invoquant des problèmes informatiques avec votre banque, en relayant des appels d'urgence impliquant vos amis et les membres de votre famille, en utilisant un langage menaçant, etc.). En cas de doutes, même mineurs, n'agissez pas: mettez fin à l'appel et vérifier soigneusement la source ou l'identité.

3 **Vérifiez attentivement la source et l'identité de l'interlocuteur:**

- Vérifiez toujours d'où proviennent les messages, les appels, les courriels et les liens - même s'ils semblent officiels, semblent provenir d'un ami ou de votre famille, 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; rechercher des erreurs d'orthographe, des URL étranges ou des indicateurs de sécurité manquants (par exemple, vérifier que le lien du site web inclut un «s» dans «HTTPS» pour s'assurer que le site web est sécurisé, et vérifier toute lettre ajoutée ou manquante dans le nom de l'entreprise).

- N'ouvrez pas de liens à partir 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 si quelqu'un avec une voix familière vous appelle avec une demande urgente d'argent et prétend être un membre de la famille (par exemple, parents, sœur / frère, enfant).

- Utilisez des coordonnées vérifiées pour contacter directement l'entreprise ou l'individu et ne vous fiez jamais aux coordonnées fournies par le fraudeur présumé (par exemple, recherchez le nom de l'entreprise de manière indépendante, utilisez des annuaires commerciaux vérifiés, recourez à des méthodes de contact précédemment confirmées). Les escrocs peuvent prétendre être autorisés ou imiter le site Web 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'IOSCO (↖). Pour les fournisseurs de cryptos, vérifiez s'ils sont agréés dans l'UE (par exemple, vérifiez le registre de l'AEMF (↖).

4 **Faites attention aux astuces potentielles en matière d'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 les appareils et les comptes:**

Utilisez des mots de passe forts et uniques, gardez-les secrets et évitez de réutiliser les mêmes informations d'identification sur différentes plates-formes. Activez l'authentification multi-facteurs dans la mesure du possible. Quelques conseils sur les mots de passe sont disponibles ici (↖). Gardez votre logiciel et votre protection antivirus à jour et activés.

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

Si cela semble trop beau pour être vrai, c'est que 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 de précieuses sources de connaissances pour les fraudeurs. Révéler trop de choses sur vous-même 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:

Pour bloquer tout autre transfert vers des comptes suspects et éviter des pertes supplémentaires. Arrêtez tout contact avec les escrocs – ignorez leurs appels et leurs courriels et bloquez l'expéditeur.

Contactez votre banque ou institution financière:

Informez immédiatement votre banque ou votre institution financière via les canaux de contact officiels, afin d'explorer les options de gel des capitaux ou d'annulation des transactions.

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

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 : assurez-vous de les changer tous, afin que les fraudeurs ne puissent pas les réutiliser.

Signalement et alerte:

Signalez l'incident à la police ou à votre autorité financière nationale ( ) et informez votre réseau (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 au recouvrement de fonds:

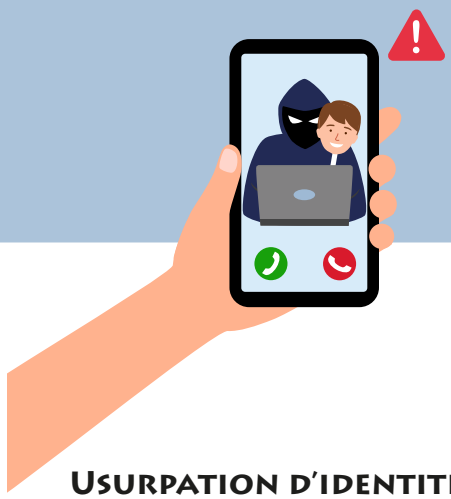
Le fraudeur peut vous contacter en sachant que vous êtes victime d'une escroquerie antérieure, prétendant être une autorité publique (par exemple, la police, l'autorité fiscale ou financière, etc.) et offrir de récupérer votre argent perdu moyennant des frais. C'est souvent une autre tentative de vous arnaquer. Rappelez-vous que, malheureusement, avoir été la victime d'une arnarque 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 *deep fakes*

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.), un distributeur d'assurances, une société informatique ou même un membre de votre famille. L'appelant peut vous exhorter à transférer des fonds pour les garder en sécurité, citant une activité suspecte sur votre compte ou votre police d'assurance. Ils peuvent également vous demander de divulguer vos coordonnées bancaires (par exemple, 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 peut résoudre rapidement le problème. L'appelant peut utiliser un numéro falsifié, correspondant souvent au numéro de téléphone de votre banque pour paraître légitime (usurpation d'identité).

Les escrocs peuvent utiliser l'IA pour créer 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. **Il est connu sous le nom de «Deepfake».**

Ce qui pourrait arriver:

En mentionnant des données personnelles et en créant un sentiment d'urgence, l'escroc vous incite à entreprendre des démarches que vous n'aviez pas l'intention de réaliser, telles que l'envoi d'argent sur un compte, le clic sur un lien malveillant ou l'installation d'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 peut changer votre mot de passe, accéder à votre compte bancaire et voler votre argent. Rappelez-vous : le simple fait qu'un appelant connaisse certaines de vos informations personnelles ne signifie pas qu'il est digne de confiance.

Phishing et ingénierie sociale

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

Les escrocs utilisent l'IA pour créer des messages de phishing convaincants en analysant les données des médias sociaux pour identifier leurs victimes et en adaptant le contenu pour 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 l'assurance

Vous voyez une publicité sur les réseaux sociaux ou un site web faisant la promotion d'une «possibilité d'investissement à durée limitée à faible risque» ou d'une «remise à durée limitée» sur une assurance d'une entreprise bien connue. L'annonce présente une photo d'une célébrité et/ou des recommandations, qui sont souvent fausses. 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 d'aspect professionnel. Vous êtes encouragé à investir un petit montant - qui sera suivi plus tard de demandes de sommes plus importantes - , ou à payer la prime dans ce qui semble être un compte sécurisé.

Les fraudeurs utilisent des outils d'IA pour rendre ces fausses propositions ou courriels très convaincants et difficiles à détecter. Ils utilisent également des robots de réseaux sociaux alimentés par l'IA pour créer de faux comptes qui interagissent avec vous, diffusent des informations erronées et simulent des comportements réels pour gagner votre 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 alors que l'entreprise n'existe pas ou que le risque n'est pas couvert par l'assurance. 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 qui pourraient vous conduire à perdre encore plus d'argent).

Arnaque aux sentiments

Vous avez été contacté sur les réseaux sociaux, les applications de rencontres, ou par téléphone / message par quelqu'un que vous n'avez pas rencontré dans la vie réelle. Cette personne s'engage dans des conversations fréquentes, personnelles et romantiques, construisant insidieusement une confiance mutuelle en utilisant de faux profils. Peu à peu, la conversation s'oriente vers l'argent ou la présentation d'opportunités financières prétendant d'énormes bénéfices liés à des investissements en crypto-actifs et vous encourageant à investir dans des offres promettant des rendements élevés et de faible risque. Ils vous guident à travers la création d'un compte et le versement d'un petit dépôt initial pour que le système semble réel.

Les fraudeurs utilisent l'IA pour générer de faux profils, pour identifier leurs victimes sur les réseaux sociaux et les applications de rencontres à l'aide des données que vous avez rendues publiques, ou pour créer des messages via des chatbots.

Ce qui pourrait arriver:

L'escroc retire autant d'argent que possible depuis votre compte, puis coupe toute communication et disparaît. Le site internet ou l'application d'investissement frauduleux est mis hors ligne, vous laissant sans accès aux investissements supposés. Dans certains cas, les escrocs peuvent utiliser les informations obtenues au cours de l'arnaque pour cibler vos amis et votre famille et commettre une usurpation d'identité qui peut avoir des conséquences financières ou juridiques pour vous (par exemple, le fraudeur peut vérifier les portefeuilles volés à votre nom et vous pourriez être tenu responsable des dettes ou des crimes commis sous votre nom jusqu'à preuve du contraire).

Achat d'escroquerie

Vous rencontrez une offre attrayante pour un achat en ligne. La société proposant l'opération demande un paiement en dehors d'une plateforme officielle, affirmant qu'elle utilise 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 son design, de sorte que vous entrez vos coordonnées bancaires en ligne pour effectuer le paiement.

Les escrocs utilisent l'IA pour créer de faux sites Web bancaires, des factures et des messages de confirmation de commande très convaincants. 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'accord plus crédible.

Ce qui pourrait arriver:

Le paiement via un lien tiers contourne les protections du système de paiement ordinaire. L'escroc obtient vos informations de connexion à votre compte bancaire et vole votre argent.