Image not found or type unknown

Les nouvelles escroqueries à l'ère numérique

Actualité législative publié le **26/01/2025**, vu **118 fois**, Auteur : Yanis MOUHOU

Les nouvelles escroqueries numériques, dans les domaines des cryptomonnaies, des applications mobiles et des réseaux sociaux, créent des défis importants pour les régulateurs et les législateurs

Introduction : L'Émergence de Nouvelles Escroqueries à l'Ère du Numérique

À mesure que les technologies numériques évoluent, le monde du **cybercrime** s'adapte rapidement, donnant naissance à de nouvelles formes d'escroqueries. Ces escroqueries, qui tirent parti de l'usage omniprésent d'Internet, des **cryptomonnaies**, des **réseaux sociaux**, des **applications mobiles** et des **technologies de la blockchain**, constituent des menaces croissantes pour les consommateurs et les entreprises à l'échelle mondiale. Si les fraudes numériques existent depuis les premiers jours d'Internet, leur sophistication et la diversité des techniques utilisées rendent leur détection, leur prévention et leur répression de plus en plus complexes.

Cet article explore les **nouvelles escroqueries numériques** qui ont émergé avec l'essor des technologies modernes, en particulier dans les domaines des **finances décentralisées (DeFi)**, des **cryptomonnaies**, des **applications mobiles**, et des **réseaux sociaux**, tout en analysant les réponses juridiques possibles pour contrer ces menaces.

I. Les Nouvelles Escroqueries Numériques : Typologie et Méthodes

1.1. Escroqueries et Fraudes Cryptographiques

Les **cryptomonnaies** et la **blockchain** ont ouvert un nouveau terrain pour les escrocs. Si ces technologies offrent des avantages considérables en termes de décentralisation et de sécurité, elles sont également exploitées pour commettre des **escroqueries** complexes et difficiles à détecter.

1. **Fraudes ICO (Initial Coin Offering)** : Les **Initial Coin Offerings** (ICO) sont des mécanismes par lesquels des entreprises collectent des fonds pour financer des projets liés aux cryptomonnaies. Cependant, de nombreux escrocs utilisent cette méthode pour **lancer des projets fictifs**, en promettant de fortes retombées financières avant de disparaître avec l'argent des investisseurs. Ces arnaques sont souvent qualifiées de **"exit scams"**.

- **Exemple :** Le projet **BitPetite**, une ICO qui a levé plusieurs millions de dollars avantde fermer sans livrer aucun produit.

2. **Rug Pulls dans la Finance Décentralisée (DeFi)** : La **DeFi** permet aux utilisateurs de prêter, emprunter, échanger et investir dans des actifs numériques sans avoir recours à des intermédiaires traditionnels comme les banques. Toutefois, certains projets DeFi sont des arnaques où les créateurs lancent des projets en promettant de bons rendements, puis retirent les fonds investis en une seule transaction avant de fermer la plateforme.

    - **Exemple : PizzaToken**, qui a attiré des investisseurs avant de disparaître avec l'argent de ses utilisateurs.

3. **Phishing et Hameçonnage via des Portefeuilles Crypto** : Le **phishing** reste une méthode courante pour voler des fonds en cryptomonnaies. En imitant des plateformes légitimes d'échange de cryptomonnaies, les fraudeurs volent les **clés privées** des utilisateurs, leur permettant de siphonner les fonds présents sur leurs portefeuilles.

    - **Exemple :** En 2020, un site de phishing imitant **Coinbase** a piégé des milliers de personnes et a conduit à la perte de **plus de 20 millions de dollars**.

1.2. Escroqueries dans le Domaine des Applications Mobiles

Les **applications mobiles** sont un terrain fertile pour les escrocs. Les utilisateurs de smartphones sont souvent exposés à des escroqueries sous forme d'applications **falsifiées** ou de logiciels malveillants. Ces applications peuvent être des **applications de paiement** contrefaites ou des **jeux mobiles** qui collectent les informations personnelles des utilisateurs à leur insu.

1. **Applications de Pseudo-Paiement :** Ces applications prétendent offrir des services de **transfert d'argent** ou de **paiement de factures**, mais une fois les informations bancaires saisies, l'escroc s'en empare.

    - **Exemple :** Des milliers de faux **portefeuilles de cryptomonnaies** sur Android et iOS ont permis de détourner des fonds, simplement en accédant aux informations des utilisateurs.

2. **Applications de "Crypto-faucets" Frauduleuses :** Certaines fausses applications promettent des **gains en cryptomonnaies** (comme le Bitcoin ou l'Ethereum) en échange d'actions simples, mais en réalité, elles volent les informations de paiement ou des **réseaux privés virtuels** (VPN).

    - **Exemple :** Une application prétendant offrir des récompenses en Bitcoin, mais qui dérobe en fait les informations bancaires des utilisateurs pour effectuer des virements.

1.3. Escroqueries sur les Réseaux Sociaux

Les **réseaux sociaux** sont un vecteur idéal pour les fraudeurs. Ils exploitent l'influence d' **influenceurs** ou utilisent des **publicités trompeuses** pour arnaquer les utilisateurs.

1. **Escroqueries par Investissements fictifs** : De faux comptes et **publicités sponsorisées** sur des réseaux sociaux comme Instagram ou Twitter font la promotion de projets fictifs ou

Copyright © 2025 Légavox.fr - Tous droits réservés

de **programmes d'investissement**. Ces arnaques sont souvent déguisées sous des **promesses de rendements élevés**.

    - **Exemple :** Des célébrités comme **Kim Kardashian** ou **Floyd Mayweather** ont été accusées de promouvoir des ICO frauduleuses sur leurs comptes de réseaux sociaux.

2. **Arnaques à la "Fake Giveaway"** : Cette méthode consiste à promouvoir des **concours** ou des **tirages au sort** fictifs, souvent liés à des cryptomonnaies, où les utilisateurs sont invités à envoyer des fonds pour participer à un tirage au sort en pensant qu'ils gagneront un prix substantiel.

    - **Exemple :** De fausses promotions de **Bitcoin giveaways** ont été utilisées par des escrocs se faisant passer pour des entreprises de confiance pour siphonner des milliers de dollars.

II. Les Réponses Juridiques aux Escroqueries Numériques : Enjeux et Perspectives

2.1. La Régulation des Cryptomonnaies : Un Cadre Juridique Émergent

Face à la prolifération des escroqueries dans le secteur des cryptomonnaies, plusieurs pays ont introduit des régulations spécifiques pour encadrer les **ICOs**, les **plateformes d'échange** et les **actifs numériques**. L'Union Européenne, par exemple, travaille sur la régulation des cryptomonnaies via la directive **MiCA** (Markets in Crypto-Assets), qui vise à créer un cadre harmonisé pour les actifs numériques tout en prévenant les abus et les fraudes.

- **Régulations existantes :** Aux États-Unis, la **Securities and Exchange Commission** (SEC) a mis en place des régulations pour surveiller les ICOs et les cryptomonnaies, tout en poursuivant les escrocs à travers des actions judiciaires. De plus, la **Financial Action Task Force (FATF)** impose des recommandations pour que les plateformes de cryptomonnaies respectent des normes anti-blanchiment d'argent (AML) et KYC.

2.2. La Lutte Contre les Escroqueries sur les Réseaux Sociaux

La lutte contre les **escroqueries sur les réseaux sociaux** implique l'adoption de politiques de **modération** renforcées par les entreprises de médias sociaux, ainsi que l'introduction de **sanctions** contre les comptes frauduleux. Les régulations comme le **Digital Services Act** en Europe imposent aux plateformes de mieux contrôler le contenu frauduleux, mais la mise en application reste complexe.

- **Sanctions et procédures civiles :** Les victimes d'escroqueries numériques peuvent se tourner vers les tribunaux pour obtenir des réparations. En Europe, des lois comme la **Directive sur les droits des consommateurs** permettent de sanctionner les arnaques liées à la publicité en ligne.

2.3. La Responsabilité des Fournisseurs de Services Numériques

Copyright © 2025 Légavox.fr - Tous droits réservés

Les entreprises qui fournissent des services numériques, y compris les **échanges de cryptomonnaies** et les **applications mobiles**, ont une **responsabilité** accrue pour éviter les escroqueries. L'**obligation de diligence** impose à ces entreprises de mettre en place des mécanismes de sécurité et de conformité pour prévenir les fraudes.

- **Obligations de diligence :** L’obligation de vérifier les **identités des utilisateurs** (KYC) et de signaler les **activités suspectes** devient une norme pour les services en ligne, notamment dans le secteur des cryptomonnaies.

Copyright © 2025 Légavox.fr - Tous droits réservés