Arnaques sur internet. Quel recours ?

Fiche pratique publié le **05/02/2021**, vu **2670 fois**, Auteur : LFD Criminalistique

Les arnaques sur internet constituent un phénomène criminel connu depuis quelques années, mais qui monte en puissance depuis le début de la crise sanitaire liée au coronavirus. Comment les détecter ?

1. La cybercriminalité dans notre société actuelle.

2. Typologies actuelles d'arnaque en France.

3. Quelle protection juridique face aux menaces ?

1.- La cybercriminalité dans notre société actuelle.

Depuis début de la pandémie sanitaire liée au coronavirus, les cybercriminels ont compris la vulnérabilité des systèmes informatiques, obligés à fonctionner en mode télétravail, sans préavis ni délai permettant l'adoption d'un cadre sécuritaire pour les sociétés et les administrations publiques.

Mais chez les particuliers, obligés à rester cloîtrés dans leurs domiciles, souvent en chômage partiel ou en journée de travail réduite, les commerces fermés, les heures passées au quotidien sur internet se sont multipliées, ce que certains ont profité pour mettre en place toutes sortes d'arnaques astucieuses, et même pour développer les procédés déjà existants.

Dans un contexte mondial incertain et très changeant, en pleine crise sanitaire, la société doit s'adapter à de nouvelles restrictions en permanence, à de nouvelles règles, de changements des politiques sanitaires, des libertés individuelles.

Toutes ces circonstances ont été cependant anticipées et très bien exploitées par les cybercriminels et cyber-escrocs, profitant d'une période particulière de l'histoire, où toute l'humanité avait la tête ailleurs.

2.- Typologies actuelles d’arnaque en France.

Notre pays est frappé de pleins fouets par une vague sans précédent d’arnaques de tout genre, et notamment depuis quelques mois.

La plus répandue, la plus ancienne est sans doute l’arnaque aux sentiments, aussi connue en tant qu’arnaque nigérienne ou à l’ivoirienne, car ce depuis ces deux pays que les cyber-escrocs ciblent nos concitoyens.

Si bien la méthode est bien connue, l’approche change fréquemment dans le but de détourner l’attention des victimes.

Cependant, le but reste inchangé : mettre en confiance le « pigeon » dans le seul but de lui soutirer de l’argent, sous prétexte d’une fausse situation de détresse, à l’aide d’un faux profil, d’une fausse photo, d’ailleurs très difficiles à sourcer.

Cette typologie d’arnaque est très répandue sur les sites de rencontres, mais elle a été poussée bien au-delà de ses limites, faisant actuellement partie de campagnes indiscriminées de mailing, sans ciblage précis de victimes potentielles. La technique s’appuie plutôt sur la quantité que sur la qualité et le ciblage individualisé.

Ces cyber-escrocs, plus connus en tant que « brouters », mot d’origine ivoirienne, multiplient ainsi les approches de manière exponentielle, dans l’espoir d’augmenter un taux de retours plus important que dans le ciblage personnalisé.

Le procédé ivoirien a été tellement mis au point, que certains « brouters » se font passer par des officiers de police, et même par des agents d’Interpol et Europol pour venir en aide aux victimes, tout en cachant une nouvelle escroquerie sur la même victime.

Parfois, les escrocs s’en servent de faux testaments notariés, de fausses donations nécessitant d’un apport initial pour les débloquer. Ces apports sont demandés aux victimes contre une participation sur l’héritage ou la donation.

Mais la typologie d’arnaque qui connaît le plus fort développement ces derniers mois est liée aux chéquiers volés. On voit apparaître au quotidien de nouvelles offres d’emploi, même sur le site officiel de Pôle Emploi, proposant un poste très simple, pas très fatigant, mais très bien rémunéré. Le rêve de tout être humain.

La dernière en date propose un emploi de chauffeur privé en véhicule haut de gamme, au service de touristes fortunés. L’employeur offre un chèque de 1 500 euros, une sorte de fausse prime à l’emploi que la victime doit encaisser, puis reverser aux escrocs en liquide, avant que le délai de vérification de la banque émettrice ne s’écoule.

Bien entendu, les chèques sont volés et la victime perd l’intégralité du montant ainsi reversé aux escrocs, sans compter sur les dommages collatéraux qui en découlent : interdits bancaires, interdits de chéquier, etc.

La même méthode est revêtue de différents types d’offres de travail, mais le procédé reste inchangé.

Cette méthode est tout aussi utilisée par la petite délinquance, en profitant de la naïveté ou l’excès de confiance de ses victimes, généralement une connaissance occasionnelle.

Il y en a, en fin, les « pourriels » que tout internaute découvre régulièrement dans sa boîte de réception, proposant toutes sortes de gains, de retours sur investissement juteux, de dons ou de participations dans de très bonnes œuvres avec une grosse commission à la clé.

En résumé, peu importe la façon de maquiller les arnaques sur internet, elles proposent toujours un gros bénéfice au moindre effort.

Et malgré les avertissements des autorités, la diffusion de messages d’alerte dans les médias et les réseaux sociaux, les cyber-escrocs finissent toujours par trouver de nouvelles victimes.

3.- Quelle protection juridique face aux menaces.

La plupart de ces attaques malveillantes, de ces arnaques virtuelles sont lacées depuis l'étranger, ce qui rend souvent très difficile l'identification des auteures, des responsables, ainsi que leur traduction en justice sur le sol français.

Cependant, il faut impérativement déposer plainte auprès des autorités, car chaque témoignage peut fournir de nouveaux indices, permettant une éventuelle identification formelle des escrocs.

Dans le cas où l'arnaque proviendrait du même pays d'origine que la victime, les autorités et juridictions locales sont compétentes pour se saisir de l'affaire. La traçabilité des paiements est plus facile et exploitable, et les forces de l'ordre ont plus de chances de mener à terme l'enquête.

Dans la mesure du possible, il faut toujours refuser d'encaisser un chèque qu'on nous demande de rembourser en espèces. Il s'agit d'un indice évident de la provenance frauduleuse du chèque.

Si jamais un officier de police, de gendarmerie ou d'Interpol / Europol propose spontanément son assistance à la victime sur internet, il faut systématiquement se méfier.

Il est fréquent que les escrocs usurpent l'identité d'un officier de police réel, mais ils utilisent toujours une adresse mél gratuite du genre @gmail.com, hotmail.fr, @aol.com parmi d'autres, alors que les institutions policières françaises sont facilement reconnaissables grâce notamment ou domaine « @interieur.gouv.fr » ou « @gendarmerie.interieur.gouv.fr » sur l'adresse mél.

Dans tous les cas, il est fortement conseillé de consulter un avocat, car ce genre d'escroqueries relève du code pénal, ou même de soumettre les documents suspects à un expert judiciaire en écritures et documents. Ce genre de démarche est normalement gratuite, permettant la mise en évidence du faux avant de réaliser un virement suspect à l'étranger.

Par LFD Criminalistique.fr

Experts en écritures et documents