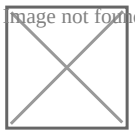

Recrutements frauduleux et usurpation d’identité.

Conseils pratiques publié le **28/01/2022**, vu **6075 fois**, Auteur : LFD Criminalistique

Les fausses offres d'embauche se multiplient sur internet. L'identité des victimes, souvent très fragiles est usurpée et les conséquences deviennent parfois insurmontables.

1.- Comment reconnaître une fausse offre d’emploi ?

Depuis quelques années, les fausses offres d’embauche se multiplient sur internet, tant sur des sites privés comme chez Pôle Emploi.

Malgré la mise en garde permanent des autorités, les cybercriminels et petits escrocs mettent en ligne des offres de plus en plus attrayants, dans le but de récolter les données personnelles des candidats, mais parfois aussi pour encaisser des chèques bancaires dérobés.

Ces fausses offres d’emploi présentent plusieurs caractéristiques communes, permettant une identification rapide de la fraude.

D’une manière générale, les offres ne demandent aucune expérience professionnelle préalable, en échange d’une rémunération bien trop élevée, souvent accompagnée de d‘autres avantages pour le salarié.

Ces conditions professionnelles sont souvent proposées dans le cadre d'un emploi à domicile. Les escrocs savent qu'un bon salaire sans bouger de chez soi est toujours attractif, quelle que soit l'activité demandée.

Les offres frauduleuses d'emploi peuvent présenter aussi la forme de messages électroniques, usurpant l'identité d'une société ou d'un organisme bien réel. Ces courriels sont normalement bien structurés et sophistiqués, portant le logo d'une grande enseigne et même celui de Pôle Emploi.

Reconnaître ce type d'offres frauduleuses est très simple, car elles demandent toujours de renvoyer au soi-disant employeur des données personnelles et financières sensibles, ainsi que de formulaires et de pièces fictives liées à l'embauche ou même les coordonnées bancaires.

Un site officiel est disponible pour signaler ce genre d'activité criminel : https://www.internet-signalement.gouv.fr/

2.- Les bons réflexes à adopter face à une proposition suspecte.

Lorsqu'une proposition d'embauche semble douteuse, plusieurs mesures doivent être respectées pour se protéger face à une tentative d'arnaque ou d'usurpation d'identité.

Certaines données personnelles, très prisées des escrocs ne sont jamais demandées par un employeur préalablement à l'entretien d'embauche, moins encore sur internet, car il s'agit d'informations sensibles : le numéro de sécurité sociale ou celui du permis de conduire, le RIB, le numéro de carte bancaire ou les accès de connexion bancaire, parmi d'autres.

Mais les plus dangereuses sont les données contenues dans les photocopies des pièces d'identité et les informations bancaires, car elles facilitent en grande mesure une éventuelle usurpation d'identité.

Une demande très en vogue en ce moment consiste à faire encaisser un chèque bancaire au demandeur d'emploi, pour ensuite retourner le montant aux faux recruteurs depuis un bureau de transfert d'argent du genre Western Union, MoneyGram ou MoneyTransfert. Il s'agit sans doute

d’un chèque volé, car aucune société ne fait pas de paiements aux futurs employés.

Si le prétendu employeur demande un paiement préalable au début de l’activité professionnelle, il s’agit sans conteste d’une escroquerie, même si le paiement est justifié par les frais d’un équipement de travail, d’une formation obligatoire ou la location d’une voiture.

Les offres d’emploi non sollicitées et reçues par messagerie électronique sont normalement adressées à escroquer les destinataires. Il ne faut surtout pas répondre.

En cas de doute, internet nous permet aujourd’hui de vérifier l’existence et souvent le sérieux d’une société, d’un employeur, si les propos ou la méthode d’embauche nous semblent suspects.

3.- Que faire si vous êtes victime d’une arnaque ou d’une usurpation d’identité ?

Les emplois très simples et très bien payés n’existent pas. Si l’offre d’emploi est trop attractive, elle est probablement frauduleuse. Il faut se méfier.

Les annonces contenant des fautes d’orthographe ou qui demandent de répondre à une adresse de messagerie gratuite, genre @gmail.com, @hotmail.fr ou @aol.com entre autres, sont normalement frauduleuses. Une véritable offre d’emploi comporte une adresse de messagerie institutionnelle : @pole-emploi.fr, @sociétéXXX.fr, etc. Vérifiez que le nom de domaine correspond à celui du site du recruteur.

En cas de soupçon, il ne faut jamais faire ni accepter un paiement avant de rencontrer le recruteur et de signer le contrat de travail.

Une éventuelle vérification de la société ainsi que des informations contenues sur le contrat de travail peut s’avérer très utile pour démasquer une tentative d’escroquerie.

Plusieurs sites officiels permettent la vérification rapide de ces informations, notamment www.infogreffe.fr, www.numero-siret.com, www.avis-situation-sirene.insee.fr ou www.service-public.fr

.

Lorsque le recruteur contacte le candidat à un horaire atypique, où qu'il refuse de rencontrer le futur employé sous prétexte d'être à l'étranger, il faut se méfier.

Si la tentative d'arnaque à l'emploi est toujours en cours, le bon réflexe est d'interrompre toute communication avec soi-disant recruteur. Une lecture attentive du dossier permet souvent de repérer assez d'incohérences pour confirmer la tentative de fraude.

Si vous avez transmis des données personnelles sensibles, prévenez votre banque, vérifiez les derniers mouvements sur votre relevé de compte et faites le nécessaire pour sécuriser les accès ainsi que l'utilisation de vos cartes bancaires, le cas échéant.

4.- Les conséquences et les risques.

Cette activité criminogène présente un point commun de départ, la fausse proposition d'embauche, mais le but est différent en fonction du type d'escroc concerné, tout comme les conséquences sur la victime.

L'escroquerie est toujours présente. Elle est définie par l'***article 313-1 du code pénal*** comme le fait, soir par usage d'un faux nom ou d'une fausse qualité, soit par abus d'une qualité vraie, soit par emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Cependant, d'autres risques sont bien présents, tel le vol de données personnelles, l'usurpation d'identité ou le faux et usage de faux, pour évoquer les plus courants.

L'usurpation d'identité est définie dans l'***article 226-4-1 du code pénal*** comme le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données et toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération.

L'usurpation d'identité est le risque le plus redouté de la victime, car consciente du vol, elle ne sait

jamais à qui ces informations ont été transmises, cédées ou vendues ou à quoi elles vont servir. Moins encore, à quoi elles vont servir dans le futur, pas forcément proche.

Par LFD Criminalistique.fr

Experts judiciaires en écriture et analyse de documents