



Arnaque aux fausses offres d'emploi : faux employeurs et faux chèques.

publié le 16/02/2018, vu 82894 fois, Auteur : [LFD Criminalistique](#)

Des fausses offres d'emploi très séduisantes prolifèrent sur internet avec une arnaque au faux chèque bancaire à la clé. Avoir les bons réflexes peuvent éviter de devenir victime.

1.- Une méthode bien rodée.

Depuis quelques années, on peut retrouver sur internet des offres d'emploi très intéressantes, proposant des contrats à durée indéterminée ainsi que des salaires très séduisants et peu adaptés aux postes évoqués ou aux compétences quasi inexistantes requises chez les candidats.

L'offre le plus fréquent reste celle du magasinier, de la vendeuse, ou des activités à domicile, sans un parcours spécial ni formation requise au préalable.

Normalement, ce genre d'offres propose des salaires à plusieurs milliers d'euros, de deux à trois fois le salaire minimum de croissance (SMIC), étant celui-ci le salaire de référence pour les postes proposés.

Ces faux employeurs n'hésitent pas à passer des annonces même chez Pôle Emploi, sous une couverture juridique fictive mais tout à fait légitime en apparence, car le temps nécessaire pour repérer ce genre de fraude dépasse largement le délai d'exécution et de mise en place de l'arnaque, se déroulant sous quelques jours.

Les candidats répondent à l'offre par mél. Les faux employeurs ne rencontrent jamais les candidats en personne, sous n'importe quel prétexte : déplacements professionnels, empêchements personnels, etc.

Tout se passe par mél ou par téléphone. L'employeur communique sa décision d'embauche au candidat et celui-ci accepte de bonne foi s'en hésiter. Ensuite la société envoie un faux chèque de quelques milliers d'euros au nouveau salarié, dans le but de financer l'achat de la soi-disant tenue de travail, une sorte de prime à l'emploi, etc.

Le faux employeur sait que la banque nécessite de quelque deux à trois semaines pour détecter et bloquer le chèque encaissé, étant toujours faux ou volé. Pendant ce temps, le faux employeur demande le remboursement de la somme versée à la victime par mandat cash, prétextant un changement soudain de décision d'embauche : le candidat ne sera finalement pas embauché ou la somme versée n'était pas la bonne. Encore des prétextes de tout genre.

Si le candidat réalise le remboursement, il reçoit normalement quelques semaines plus tard les nouvelles de son banquier, réalisant que le chèque bancaire encaissé était un faux ou volé, frappé d'opposition.

Cette arnaque est effectuée sous de faux noms, des fausses adresses, à l'aide de téléphones portables prépayés et surtout intraçables. L'arnaqueur n'est que rarement identifié et traduit en justice.

2.- Le risque de dommages collatéraux chez les victimes.

En parallèle, les escrocs peuvent utiliser le dossier personnel fourni par le candidat, comportant toutes les informations ses personnelles, normalement présentes dans un CV (nom, prénoms, date de naissance, numéro de la pièce d'identité, numéro de la Sécurité Sociale, etc.) dans des buts tout à fait différents, car avec ces informations, ils peuvent aussi usurper l'identité du candidat en toute impunité.

Si bien chaque délinquant est spécialisé dans un milieu récurrent, un seul type ou famille de délits, parfois deux, il est fréquent que ces petits escrocs en vendent les dossiers personnels de leurs victimes à des organisations ou des malfrats plus investis dans le domaine de la criminalité documentaire, la fabrication de faux papiers, l'usurpation d'identité ou pire encore, le vol d'identité.

Pour se protéger face à ce genre d'arnaque, plusieurs bons réflexes et précautions s'imposent :

- Vérifier l'existence légale de la société sur internet, sur infogreffe ou d'autres sites de confiance.

- Toujours vérifier que l'adresse mél présente sur l'offre d'emploi appartient à la société et ou nom de domaine du site officiel de la société. Une adresse mél du genre @gmail.com, @hotmail.fr, @msn.com, @aol.com, etc. est suspecte par principe.
- Ne jamais communiquer un CV ou des information personnels à des inconnus, sans vérifier la véracité de l'annonce.
- Ne jamais accepter d'encaisser un chèque sans signer un contrat de travail au préalable conforme au droit français.

3.- La responsabilité de la banque face aux chèques volés.

À titre d'information, l'établissement bancaire n'a qu'une responsabilité très limitée dans le cadre d'un encaissement de chèque frauduleux.

La banque ne doit vérifier que la « régularité apparente » du chèque : la présence de la signature du titulaire du compte, la présence de la date, l'absence de rayures sur le support ou les encres, etc.

L'établissement bancaire est obligé par la loi (art. L.131-1-1 du Code monétaire et financier), de créditer de façon automatique la somme du chèque sur le compte, au plus tard un jour ouvré après son enregistrement.

Ensuite, le chèque est envoyé à la banque émettrice pour se faire rembourser. C'est là que les protocoles de sécurité bancaires font déclencher les alarmes, car la banque émettrice constate que le chèque est volé ou faux, tout en débitant le compte du bénéficiaire du chèque, la victime, de la même somme.

Pendant ce temps, les escrocs auront normalement perçu le remboursement en liquide de la victime et disparus dans la nature.

Par LFD Criminalistique.fr

Experts judiciaires en écritures et documents.