RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

COMPRENDRE LES RISQUES

LES PROPOSITIONS D'EMPLOI NON SOLLICITÉES

En recherche active d'emploi ou non, il peut arriver de recevoir un message non sollicité qui propose un poste ou promet d'être rapidement recruté pour une activité attractive et rémunératrice. Il s'agit, par exemple, d'un emploi à domicile qui est compatible avec une autre activité professionnelle. En pratique, les fraudeurs se font passer pour de véritables recruteurs en usurpant le nom d'une entreprise, son adresse, l'identité d'un salarié ou d'un responsable de l'entreprise ou son numéro de SIRET. Ils font miroiter un poste sans jamais avoir rencontré le demandeur d'emploi et envoient, pour renforcer leur crédibilité, des documents d'apparence officielle (contrat de travail, formulaire de candidature, etc.).

BUT RECHERCHÉ

Soutirer de l'argent ou dérober des informations personnelles (données bancaires, numéro de sécurité sociale) pour en faire un usage frauduleux.

SI VOUS ÊTES VICTIME

En cas de doute, **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR** sur sa plateforme internet-signalement.gouv.fr.

INTERROMPEZ IMMÉDIATEMENT TOUTE RELATION AVEC LE PSEUDO RECRUTEUR même si ce dernier se montre menaçant par message ou par téléphone.

Si vous avez transmis des données personnelles (numéro de sécurité sociale…), **INFORMEZ-EN L'ORGANISME CONCERNÉ** (France Travail, Assurance Maladie…).

Si vous avez transmis des informations bancaires, **INFORMEZ-EN VOTRE BANQUE ET SURVEILLEZ RÉGULIÈREMENT LES OPÉRATIONS** sur votre compte bancaire.

INFORMEZ IMMÉDIATEMENT L'ORGANISME DONT L'IDENTITÉ A ÉTÉ USURPÉE OU LE SITE D'EMPLOI QUI A DIFFUSÉ L'ANNONCE avec, si possible, son numéro de référence.

Que vous soyez victime d'une tentative d'escroquerie, d'un vol de données personnelles ou d'une escroquerie financière, **DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie, ou en écrivant au procureur de la République dont vous dépendez. Ce dépôt de plainte vous aidera dans vos futures démarches en cas d'usurpation d'identité. Il est possible de déposer une pré-plainte en ligne. Pour qu'elle soit enregistrée comme une plainte, vous devrez cependant signer cette déclaration auprès d'une unité de gendarmerie ou du service de police de votre choix.

MESURES PRÉVENTIVES

Méfiez-vous des propositions d'emploi non sollicitées. Ces propositions sont souvent envoyées à de nombreuses personnes et votre adresse de messagerie ne figure pas toujours dans le champ « destinataire » où se trouvent plusieurs noms.

Méfiez-vous d'une offre trop attractive, voire hors norme. N'hésitez pas à en parler à votre entourage ou à un professionnel de l'emploi (France Travail…).

Ne transmettez jamais à un recruteur vos données personnelles (RIB, numéro de sécurité sociale, de compte ou de carte bancaire) tant que vous ne l'avez pas rencontré.

Ne versez aucune somme d'argent à un employeur potentiel en échange d'un contrat de travail ou pour suivre une formation préalable à l'embauche.

N'achetez jamais du matériel pour le compte de l'entreprise et n'acceptez jamais de recevoir un chèque ou un virement bancaire pour effectuer des achats nécessaires à votre prise de poste.

N'acceptez aucune rétribution de votre futur employeur tant que vous n'avez pas signé le contrat de travail.

Assurez-vous de l'existence juridique (SIRET) de l'entreprise à l'origine de l'offre d'emploi.

Soyez vigilant lorsqu'un recruteur vous contacte à un horaire atypique ou s'il ne peut vous rencontrer sous prétexte qu'il est à l'étranger.

Soyez attentif aux propos du recruteur en particulier lorsque par exemple, en cours d'entretien, il vous propose un poste différent de celui mentionné dans l'annonce.

Ne poursuivez pas la communication si vous doutez de l'honnêteté de votre interlocuteur.

Prenez le temps de lire avec attention tous les documents qui vous sont communiqués et n'apposez jamais votre signature sur un document sans savoir précisément ce à quoi vous vous engagez.

Soyez attentif à l'adresse de messagerie de l'expéditeur. Par exemple, une grande entreprise vous adressera toujours un message émis depuis son nom de domaine (exemple : xx@francetravail.fr et non pas france-travail@xy.com).

N'encaissez jamais de chèque qui ne serait pas de votre employeur. Même si le montant d'un chèque déposé à votre banque apparaît en crédit sur votre compte, la banque, une fois les vérifications réalisées (chèque volé…), a plusieurs semaines pour valider l'opération ou l'annuler en débitant votre compte du même montant.

Tenez à jour votre antivirus et votre système d'exploitation.

France Travail

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Escroquerie** (article 313-1 du code pénal) : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'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* ». Ce délit est passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** (article 226-18 du code pénal): le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

- **Usurpation d'identité** (article 226-4-1 du code pénal): le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de 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, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V250110

France Travail