RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

PIRATAGE DE L'ESPACE PERSONNEL D'UN RECRUTEUR (SITE D'EMPLOI)

COMPRENDRE LES RISQUES

Le piratage de l'accès à l'espace personnel d'un site d'emploi désigne sa prise de contrôle par un cybercriminel au détriment de l'organisation professionnelle à laquelle appartient ce compte. En pratique, les cybercriminels ont pu obtenir l'accès à ce compte par différents moyens : mot de passe trop simple, communication de votre mot de passe suite à un hameçonnage ou utilisation d'un même mot de passe sur différents espaces dont l'un a été piraté. Dans le cas de l'hameçonnage, l'objet du message porte sur des sujets très divers : lutte contre la fraude, vérification de l'identité, diffusion de l'annonce, etc. En cas de non-réponse, une mesure restrictive est souvent annoncée (fermeture de votre espace personnel…).

BUT RECHERCHÉ

Récupérer les identifiants et les mots de passe d'accès à l'espace personnel pour en faire un usage frauduleux (vol de données personnelles, escroqueries financières, etc.)

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre espace, **PRÉVENEZ IMMÉDIATEMENT LE SITE D'EMPLOI CONCERNÉ** qui mettra en œuvre les mesures nécessaires.

Si vous avez encore accès à votre espace personnel, **MODIFIEZ IMMÉDIATEMENT VOTRE MOT DE PASSE** (voir notre fiche sur la gestion des mots de passe).

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS.** Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ SANS TARDER LE MOT DE PASSE COMPROMIS SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ SYSTÉMATIQUEMENT ET AU PLUS VITE le site d'emploi du piratage dont vous avez été victime si cela n'a pas été réalisé.

SI VOUS AVEZ CONNAISSANCE DE L'IDENTITÉ DES CANDIDATS CONTACTÉS PAR LE FRAUDEUR, PRÉVENEZ-LES OU FAITES-LES PRÉVENIR par le site d'emploi pour qu'ils ne donnent pas suite aux contacts suspects.

VÉRIFIEZ QU'AUCUNE PUBLICATION N'A ÉTÉ RÉALISÉE ou action vers des candidats potentiels n'ont été réalisées avec le compte piraté, en fonction des fonctionnalités du site.

Si vos coordonnées de carte bancaire étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

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

Ne communiquez jamais d'informations sensibles par messagerie, par téléphone ou sur Internet : aucun site d'emploi sérieux ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance, ou allez directement sur le site d'emploi en question par un lien favori que vous aurez vous-même créé.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message, est inhabituelle ou vide.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse pour vous tromper.

En cas de doute, contactez si possible directement le site concerné pour confirmer le message ou l'appel que vous avez reçu.

Utilisez des mots de passe différents et complexes pour chaque site et application que vous utilisez.

Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

Activez la double authentification pour augmenter le niveau de sécurité si le site vous le permet.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Déconnectez-vous systématiquement de votre espace personnel après utilisation pour éviter que quelqu'un puisse y accéder après vous.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

France Travail

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.

- **Accès frauduleux à un système de traitement automatisé de données** (article 323-1 du code pénal) : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine encourue est de cinq ans d'emprisonnement et de 150 000 euros.

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

Licence Ouverte v2.0 (ETALAB)

V260128