ACADÉMIE
DE DIJON
Liberté
Égalité
Fraternité

**Cellule de Gestion
des Ressources Humaines**

Dijon, le 15 Juin 2021

Secrétariat Général
CGRH
Affaire suivie par :
Pierre NOBLET
Tél : 03 80 44 86 44
Mél : cpf-cgrh@ac-dijon.fr

2 G rue Général Delaborde
BP 81 921
21019 Dijon cedex

Objet : Compte Personnel de Formation – Campagne d'escroquerie

Références :

- Vu le code de l'éducation,
- Vu l'article 313-1 du code pénal concernant les appropriations frauduleuses, de l'escroquerie et des des infractions voisines ;
- Vu l'article 323-1 du code pénal concernant les atteintes aux systèmes de traitement automatisé de données ;
- Vu l'article 226-4-1 du code pénal portant sur l'atteinte à la vie privée et l'usurpation d'identité ;
- Vu l'ordonnance n°2017-53 du 19 janvier 2017 portant diverses dispositions relatives au compte personnel d'activité, à la formation et à la santé et la sécurité au travail dans la fonction publique ;
- Vu la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
- Vu la loi n°2019-828 du 6 août 2019 de transformation de la fonction publique ;
- Vu la loi n°2020-1379 du 14 novembre 2020 autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire, article 13 ;
- Vu le décret n°2019-1392 du 17 décembre 2019 modifiant le décret n°2017-928 du 6 mai 2017 relatif à la mise en œuvre du compte personnel d'activité dans la fonction publique et à la formation professionnelle tout au long de la vie ;

Des campagnes d'escroqueries ont été identifiées ces derniers mois et sont toujours en cours. La Caisse des dépôts, membre du dispositif Cybermalveillance.gouv.fr, et qui gère le site moncompteformation.gouv.fr, analyse cette menace et dispense ses recommandations pour y faire face.

1. Comment identifier l'escroquerie

L'arnaque au Compte Personnel de Formation démarre généralement par un appel téléphonique d'une personne prétendant appartenir à la plateforme « Mon Compte Formation », ou à un organisme de formation ou bien encore à un organisme public comme le groupe Caisse des Dépôts, le ministère du Travail, de l'Emploi et de l'Insertion ou Pôle Emploi.

L'escroc fait valoir à la victime ses possibilités de droits à la formation. Il indique que ces droits sont utilisables et mobilisables par le biais du compte CPF, qui peut être consulté et géré depuis le site Internet moncompteformation.gouv.fr. Il argumente, de manière convaincante et/ou pressante, pour que la victime s'inscrive à une formation.

Parfois, l'escroc informe la victime de son droit à transférer les heures de DIF acquises jusqu'en 2014 vers son compte CPF. Il précise que ces heures seront perdues si cette action n'est pas réalisée avant la fin de l'année et demande alors d'anciens bulletins de salaire ou justificatifs de l'employeur de l'époque nécessaires à ce transfert. Cet argument vise à crédibiliser la démarche de l'escroc puisqu'il s'agit là d'une possibilité offerte aux détenteurs de compte CPF, ce qui lui fournit un prétexte pour contacter la victime qu'il met ainsi en confiance. Cela permet également d'augmenter le crédit disponible sur le compte, et donc, d'augmenter le montant des sommes que l'escroc pourra dérober.

2. Les techniques utilisées pour accéder au compte de la personne

En pratique, l'escroc a recourt à différents stratagèmes pour parvenir à ses fins et accéder au compte CPF de la victime.

Il peut, par exemple, demander le numéro de sécurité sociale de la victime et parfois même son mot de passe qui permet l'accès au compte CPF. Il peut également accompagner la victime pour l'aider à réinitialiser son mot de passe si elle a déjà créé un compte et en profiter pour tenter de le récupérer.

Si la victime n'a pas encore procédé à la création de son espace personnel, l'escroc peut proposer de l'aider à le créer pour en obtenir les informations de connexion au compte, à savoir le numéro de sécurité sociale et le mot de passe. Parfois, il peut même aller jusqu'à le créer à sa place, en y inscrivant une adresse de messagerie (mail) qui lui appartient afin de prendre le contrôle du compte.

Dans certains cas, l'escroc connaît déjà les nom, prénom, numéro de téléphone et de sécurité sociale de la victime.

Enfin, certaines victimes ont découvert qu'elles avaient été inscrites à des formations à leur insu et débitées de leur crédit. Dans cette situation, il est très probable que leur compte CPF ait été piraté avec des informations (identité, numéro de sécurité sociale, adresse...) obtenues de manière frauduleuse.

Les auteurs de ce type d'arnaque diffusent également des publicités sur des sites Internet, des applications ou des réseaux sociaux *(Facebook, Instagram...)* ou envoient des e-mails « publicitaires » sous la forme de spams qui orientent les internautes vers un formulaire où ils renseignent leurs souhaits de formation et leurs coordonnées. Ces derniers sont ensuite appelés pour la mise en œuvre de l'arnaque.

3. Conseils de prévention

Pour utiliser son compte personnel de formation, il n'y a qu'un seul site officiel : moncompteformation.gouv.fr. Pour éviter d'être piraté, il ne faut jamais communiquer ses identifiants (numéro de sécurité sociale ou mot de passe). L'agent doit rester le seul à accéder à son compte. Dans le cas contraire, ses droits à la formation pourraient être piratés.

1. Au moindre doute, ne communiquez jamais d'informations sensibles (numéro de sécurité sociale, mot de passe) par messagerie, par téléphone ou sur Internet : Votre numéro de sécurité sociale est un numéro unique et personnel qui permet de vous identifier auprès de divers organismes publics. Il ne peut être utilisé que dans des cas bien précis et seuls des organismes habilités dans un strict cadre réglementaire sont autorisés à l'enregistrer et l'utiliser. Par ailleurs, ne communiquez jamais votre mot de passe à un tiers. Aucun organisme de formation professionnelle ou centre d'appel n'est autorisé à vous demander ces informations personnelles et confidentielles. Si l'on vous les demande, considérez que vous êtes face à une tentative d'escroquerie.

2. Changez immédiatement le mot de passe de votre compte CPF si vous l'avez communiqué. Changez également le mot de passe piraté sur tous les autres sites ou comptes sur lesquels vous pouviez l'utiliser. Cela permettra d'éviter que les escrocs piratent ces autres sites ou comptes et vous y portent également préjudice. Tous nos conseils pour gérer au mieux vos mots de passe.

3. Si vous ne pouvez plus vous connecter à votre compte CPF, signalez votre piratage et demandez la réinitialisation de votre mot de passe. Contactez la plateforme Mon Compte Formation au 09 70 82 35 51 (du lundi au vendredi de 9h00 à 17h00 – appel non surtaxé – choix 1 puis 6 sur le serveur vocal interactif) afin de l'informer du piratage de votre compte et demander la réinitialisation de votre mot de passe.

Secrétariat Général
CGRH
Affaire suivie par :
Pierre NOBLET
Tél : 03 80 44 86 44
Mél : cgrh@ac-dijon.fr

2 B rue Général Delaborde
BP 61 321
21019 Dijon cedex

4. Mettez fin sans tarder à la communication téléphonique. Stoppez toute communication au moindre doute, même si votre interlocuteur se montre insistant ou menaçant. Au besoin et si possible, bloquez le numéro de téléphone de l'appelant. Votre appareil dispose en effet de fonctionnalités permettant de bloquer des numéros de téléphone. Conservez toutes les preuves en votre possession : nom de la formation, nom de l'organisme de formation, adresse postale, adresse mail, numéro de téléphone, contrats de formation, etc.

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

6. Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

7. Signalez les faits à la plateforme Mon Compte Formation : si vous constatez que vous avez été inscrit à une formation à votre insu, signalez les faits sur le site moncompteformation.gouv.fr , dans la rubrique « Que dois-je faire ? », au point 4 « Signaler l'escroquerie ».

8. Si vous avez été victime d'une escroquerie, déposez plainte au commissariat de police ou de la brigade de gendarmerie dont vous dépendez. Vous pouvez également adresser votre plainte par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession.

4. Liens utiles :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagnes-escroqueries-compte-personnel-formation-cpf

https://www.moncompteformation.gouv.fr/espace-public/cybermalveillancegouvfr-et-la-caisse-des-depots-sassocient-pour-lutter-contre-la-fraude

Pour la rectrice et par délégation,
Le secrétaire général adjoint,
Directeur des ressources humaines

Cédric PETITJEAN

Secrétariat Général
CGRH
Affaire suivie par :
Pierre NOBLET
Tél : 03 80 44 86 44
Mél : cgrh@ac-dijon.fr

2 G rue Gabriel Oblin
BP 81 921
21019 Dijon cedex