RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

aefe
Agence pour l'enseignement français à l'étranger

FAQ AEFE - Cyberattaque ELAP -

Une application éditée par la société ELAP et utilisée par l'AEFE a fait face à un incident de sécurité, avec pour conséquence une fuite de données personnelles. Des communications ont été envoyées par l'AEFE à tous les chefs d'établissements ainsi qu'aux personnels détachés. Il a été demandé aux établissements de communiquer auprès de leurs publics (personnels de tous statuts, fournisseurs, etc.) afin de les tenir informés des mesures et bonnes pratiques à prendre. Une communication a par ailleurs été mise en ligne sur le site web de l'Agence.

L'AEFE a réalisé une Foire aux questions avec d'apporter des réponses complémentaires à tous les personnels du réseau.

En cas de questions supplémentaires, les personnels peuvent s'adresser à leurs référents RGPD.

Q : Quels sont les personnels potentiellement touchés par la fuite de données ? Détachés et/ou PDL et/ou IEN et/ou COCAC adjoints et/ou services centraux ?
R: Seuls les personnels des services centraux et les personnels détachés auprès l'AEFE ayant perçu des fonds de l'employeur AEFE (hors salaires) sont concernés par la cyberattaque.
Certains personnels de droit local peuvent être concernés s'ils ont fait l'objet d'un remboursement de frais de mission ou au travers des informations relatives à leur rémunération.

Q : Quels sont les agents des services centraux dont les données personnelles sont susceptibles d'avoir été communiquées ?
R : Sont potentiellement concernés les agents qui ont sollicité des prestations familiales, ont fait l'objet de remboursement de frais de mission, ont procédé à un remboursement d'un trop perçu sur leur rémunération

Q : Quels sont les agents du réseau détachés dont les données personnelles sont susceptibles d'avoir été communiquées ?
R : Sont potentiellement concernés les agents qui ont bénéficié de l'indemnité de changement de résidence, d'un remboursement de frais de visa, ont procédé à un remboursement d'un trop perçu sur leur rémunération.

Q : Quelles données me concernant ont été exfiltrées ?
R : L'Agence procède actuellement à un recensement de toutes les données à caractère personnel incluses dans les pièces jointes copiées afin de répondre précisément aux agents.

Q : Dois-je porter plainte ?

R : En cas d'utilisation frauduleuse de vos données personnelles divulguées, il est conseillé de déposer une plainte auprès du commissariat de police ou de la gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez (domicile).
Il est également possible de déposer une pré-plainte en ligne : https://www.pre-plainte-en-ligne.gouv.fr/. Après cette déclaration, vous devez vous rendre soit au commissariat soit à la brigade de gendarmerie pour signer votre plainte.

Dans l'hypothèse où votre appareil (ordinateur, tablette ou téléphone portable) serait bloqué et afficherait un message exigeant de l'argent pour un retour à la normale, vous êtes probablement victime de faits susceptibles d'être qualifiés d'entrave aux systèmes de traitement automatisé de données (STAD). Cette infraction est plus couramment appelée rançongiciel ou ransomware. Dans ce cas, vous pouvez porter plainte selon les mêmes modalités que celle évoquées plus haut, soit : sur place ou par courrier, ou en ligne **sur la plateforme THESEE du ministère de l'Intérieur** au lien suivant https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/plainte-en-ligne-arnaques-internet-thesee.

Pour toute information sur les ransomware ou rançongiciel, vous pourrez trouver des explications sur https://www.service-public.fr/particuliers/vosdroits/F34129

Q : Il est conseillé de prévenir la banque, est-ce utile d'informer les assurances ?
R : Oui, il est conseillé de prévenir votre banque.
Vous pouvez faire le point avec votre assurance concernant les risques cyber.

Q : Qui a des données dans ce logiciel ?
R : En complément des personnels cités, le système d'information budgétaire et comptable dispose des données des fournisseurs, clients de l'AEFE, et de certains parents et élèves du réseau.

Q : Les APE sont-elles concernées ?
R : Oui, dans la mesure où les conventions liant l'AEFE à ces associations sont une pièce justificative à un paiement ou à un encaissement suite à facturation par l'AEFE.

Q : Les parents et les élèves sont-ils concernés ?
R : A priori non, dans la mesure où seule la base élèves détient les informations relatives au représentant légal de l'élève.
Voici les informations qu'il peut y avoir au sein des pièces jointes dans la base ELAP sur les élèves :
Nom/Prénom/Date de naissance/Payeur/Classe

Il s'agit d'information que l'on peut retrouver sur :
- les bordereaux de droits constatés qui peuvent être attachés aux facturations,
- les fiches quotidiennes d'encaissement pour justifier des opérations diverses de compte à compte,
- les listes arrêtées de voyages scolaires
- les notifications d'attribution ou PV de commission de caisse de solidarité

Q : Quelles applications sont concernées ? Pro et/ou perso ? Si pro, lesquelles ? Seulement les applications AEFE ou également la suite Index Education, les ENT, etc. ? Les accès à des sites web sont-ils concernés ?
R : Seul le serveur de pièces jointes incluses dans l'application ELAP Finance a fait l'objet de cette intrusion informatique.

Q : L'accès à certaines applications de l'AEFE a été bloqué pendant plusieurs jours, pourquoi ?
R : Suite à la cyberattaque, l'AEFE et le MEAE ont mis en place des analyses et tests sur ces applications afin de vérifier leur sécurité et au besoin la renforcer. L'accès à ces applications est de nouveau opérationnel depuis le 6 décembre 2023, garantissant une utilisation en toute sécurité

Q : Cette attaque aurait-elle une incidence sur la mise en paiement des salaires ?
R : Cette attaque n'a aucune incidence sur la mise en paiement des salaires des personnels (services centraux comme réseau).

Q : Comment s'explique le caractère tardif de l'information ?
R : La notification à la CNIL s'est effectuée dans le temps réglementaire. L'Agence a informé les usagers d'ELAP dès le 5 novembre sur l'indisponibilité du système d'information. L'Agence a eu confirmation par ELAP de l'exfiltration des fichiers, suite à la publication par les cyberattaquants de tous les documents sur le *darkweb* le 19 novembre et a communiqué à partir du 20 novembre auprès des publics concernés.

Q : Qui contacter pour exercer votre demande de droit à l'information, et d'accès de vos données personnelles ?
R : Si vous êtes un personnel des services centraux de l'AEFE, il convient de contacter directement le Délégué à la protection des données de l'AEFE dpo.aefe@diplomatie.gouv.fr
Si vous êtes un personnel d'un établissement en gestion directe ou conventionné, vous devez contacter directement le référent RGPD de votre établissement.

Q : Que pourraient potentiellement faire les hackers de ces informations ?
R : Une utilisation malveillante des données personnelles, une usurpation d'identité, une fraude, des mouvements bancaires suspects, une atteinte à la réputation, une perte de la confidentialité des données, des appels téléphoniques suspects, une tentative d'hameçonnage.

Q : Comment vérifier tous les comptes bancaires qui sont rattachés à votre nom ?
R : Vous pouvez vous connecter sur ce site https://www.service-public.fr/particuliers/vosdroits/F2233, avec France Connect (Impôts, AMELI, etc.), cela permet de vérifier toutes les ouvertures de comptes bancaires à notre nom.
Connectez-vous régulièrement ces prochaines semaines pour vérifier qu'aucun compte à votre nom n'a été ouvert dans une autre banque. Vous pourrez en cas de mouvement frauduleux le signaler directement à votre banque.

Q : Dois-je faire refaire mes documents d'identité (passeport, CNI) ?
R : Dès lors qu'aucun fait d'usurpation d'identité n'a été constaté, il n'est pas nécessaire de refaire faire ses documents d'identité.
L'usurpation d'identité se définit comme « l'*utilisation d'informations personnelles permettant d'identifier une personne à son insu pour réaliser des actions frauduleuses*».
En cas d'utilisation frauduleuse de votre identité, vous pouvez déposer une plainte pénale : rassemblez toutes les preuves et déposez plainte au commissariat de police ou à la brigade de gendarmerie ou par écrit au procureur de la République du tribunal judiciaire dont vous dépendez (voir question « *Dois-je déposer plainte ?* »).
Une fois la plainte déposée, vous pouvez demander à faire annuler et renouveler vos pièces d'identité.
Pour toute information sur la conduite à tenir en cas d'usurpation d'identité :
https://www.economie.gouv.fr/particuliers/protection-usurpation-identite
file:///D:/donnees/uti/prive/Documents/moussys/internet/230417_FicheReflexe_UsurpationIdentite_Particuliers.pdf

Q : Que pouvez-vous faire si vous êtes concerné par une cyberattaque ?
R : L'hameçonnage (phishing) ou l'usurpation d'identité

L'hameçonnage consiste à vous envoyer un courriel ou SMS frauduleux qui vous paraîtra plus réaliste du fait de l'utilisation des données récupérées grâce à la fuite de données (un soi-disant courriel de votre médecin ou de la sécurité sociale par exemple).
N'ouvrez surtout pas les pièces jointes, n'y répondez pas, ne consultez pas les liens et supprimez le message immédiatement. Pour repérer une tentative d'hameçonnage dans votre messagerie, et pour vous prémunir contre l'usurpation d'identité en ligne, soyez vigilants :

- vérifiez que le message/courriel vous est réellement destiné ;
- faites attention aux expéditeurs inconnus ;
- soyez attentif au niveau de langage du courriel ;
- vérifiez les liens dans le courriel ;
- méfiez-vous des demandes étranges et ne transmettez rien de confidentiel ;
- portez une attention particulière sur l'adresse de messagerie source.

Recommandations de cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Si vous pensez être victime d'une usurpation d'identité à la suite de la divulgation d'informations vous concernant, vous pouvez :

- vous rendre sur le site cybermalveillance.gouv.fr pour obtenir des conseils : https://www.cybermalveillance.gouv.fr/bonnes-pratiques
- déposer plainte au plus vite auprès d'un commissariat de police ou de gendarmerie ;
- consulter les recommandations de la CNIL « Comment réagir face à une usurpation d'identité ? ».

D'une manière générale, soyez vigilant lorsque vous saisissez des données sur le web ou lorsque vous recevez des courriels vous demandant de fournir ou de mettre à jour des données vous concernant.
Afin de limiter les risques, vous pouvez adopter quelques gestes simples :

- changez vos mots de passe des services web que vous utilisez :
    - en privilégiant des mots de passe forts ;
    - en priorisant les services les plus importants (courriel, impôts, banques, sites de commerce en ligne, etc.) ;
- évitez l'utilisation d'un même mot de passe pour différents services ;
- utilisez les authentifications multi facteurs quand elles vous sont proposées par des services de confiance (par exemple l'envoi d'un SMS à usage unique sur votre téléphone pour valider une connexion).