



Communication relative à un incident de sécurité

23 octobre 2025

Conformément à nos obligations légales et par souci de transparence, nous souhaitons vous informer d'un incident de sécurité qui a récemment affecté nos systèmes d'information.

Le 20 octobre 2025, la Fédération Française de Tir a détecté une intrusion non-autorisée sur son système d'information ITAC. Cette intrusion a eu lieu entre le 18 octobre et le 20 octobre 2025.

Dès que l'incident a été identifié, et afin d'éviter toute propagation, nous avons mis en place les mesures de sécurité nécessaires et les serveurs ITAC et EDEN ont été déconnectés.

Nous avons également prévenu l'ensemble des autorités compétentes, notamment l'ANSSI et la CNIL, et avons déposé plainte.

Accompagnés d'experts, nous avons enquêté au cours des derniers jours afin d'identifier l'origine de l'incident. Les investigations ont permis de corriger la situation.

L'incident est désormais clos et les systèmes seront donc remis en service de manière sécurisée dans les prochaines heures.

L'incident pourrait avoir conduit à la fuite de données personnelles de certains membres de la FFTir. A ce titre, nous vous recommandons de rester particulièrement vigilants face à d'éventuels emails, SMS ou appels suspects vous demandant des informations personnelles et de surveiller tous comportements suspects ou activité inhabituelle.

En raison des mesures de sécurité que nous avons mises en place, à votre prochaine connexion, vous devrez obligatoirement réinitialiser votre mot de passe avec la fonction « Vous avez oublié votre mot de passe ? ». Le QRCode de votre licence actuelle a été également invalidé. Vous devrez donc télécharger à nouveau votre licence.

Nous comprenons l'inquiétude que cette situation peut générer et nous vous présentons nos sincères excuses pour les désagréments causés.

Afin de prévenir toute nouvelle intrusion malveillante, nous travaillons actuellement au renforcement de la sécurisation de nos systèmes d'information et avons décidé de lancer un audit complet de notre infrastructure.

Soyez assurés que la sécurisation optimale de vos données est une priorité pour la Fédération Française de Tir.

Quelles données sont concernées ?

Nos investigations ont permis de lister les données concernées par l'incident.

Il s'agit du numéro de licence, de l'état-civil, de l'adresse postale, de l'adresse mail et du numéro de téléphone renseignés.

Aucune donnée médicale ni aucune coordonnée bancaire n'est concernée.

La Fédération Française de Tir ne disposant pas de données relatives à la détention d'armes, celles-ci ne sont pas non plus concernées.

Qui contacter si vous avez des questions ?

Pour toute question concernant cet incident, vous pouvez contacter :

Ligne d'assistance dédiée :

- incident-itac@fftir.org
- Courrier postal : DPO FFTir, Incident ITAC, 38 rue Brunel 75017 PARIS

Notre délégué à la protection des données (DPO) :

- Email : dpo@fftir.org

Si besoin nous vous invitons à consulter les ressources présentes sur le site Assistance aux victimes de cybermalveillance | Site Officiel.

Vous pouvez également exercer vos droits ou déposer une réclamation auprès de la CNIL : www.cnil.fr

Cordialement,

Le Président

Hugues Senger

FAQ

Connaissez-vous l'origine exacte de l'incident ?

Le 20 octobre 2025, la Fédération Française de Tir a détecté une intrusion non-autorisée sur son système d'information. Cette intrusion non-autorisée a eu lieu entre le 18 octobre et le 20 octobre 2025. Dès que l'incident a été identifié, et afin d'éviter toute propagation, les mesures de sécurité nécessaires ont été mises en place et l'ensemble des systèmes d'information ont été déconnectés.

Accompagnés d'experts, la Fédération Française de Tir a enquêté au cours des derniers jours et a pu identifier très rapidement l'origine de l'incident et corriger la situation.

L'incident est désormais clos et les systèmes seront donc remis en service de manière sécurisée dans les prochaines heures.

A date, les données concernées par l'incident sont susceptibles d'avoir été compromises. L'enquête est toujours en cours pour le déterminer.

Quelles sont les données concernées par l'incident ?

Dans la mesure où nous ne les possédons pas, aucune donnée concernant la détention ou non d'arme au domicile des licenciés n'est concernée. Les données susceptibles d'avoir été compromises ne permettent donc pas de savoir si le licencié dispose d'une arme à son domicile ou non.

Aucune donnée de santé ou bancaire n'est concernée.

D'après les premières conclusions de l'enquête, l'information du club d'appartenance des affiliés n'est pas non plus concernée.

Les données concernées sont : numéro de licence, état-civil, adresse postale, adresse mail, numéros de téléphone renseignés.

Ces données sont à ce stade susceptibles d'avoir été compromises. Mais l'enquête est toujours en cours pour le déterminer.

Les demandes d'autorisation préalable sont-elles concernées ?

Non, l'incident ne concerne pas les données concernant les demandes d'autorisation préalable.

Combien de personnes sont concernées par la fuite de données ?

Nous alertons l'ensemble de nos licenciés – actifs et non-actifs.

A ce stade, les données concernées sont susceptibles d'avoir été compromises. Mais l'enquête est toujours en cours pour le déterminer.

Comment puis-je savoir si je suis concerné par l'incident et si mes données ont été piratées ?

A ce stade, les données concernées par l'incident sont susceptibles d'avoir été compromises. L'enquête est toujours en cours pour le déterminer.

La FFTir appelle donc tous les licenciés actifs et non-actifs à la prudence.

Qu'entendez-vous par "état civil" ?

Il s'agit du nom, du prénom, de la date et de la ville de naissance. Cela ne comporte pas de reproductions de documents officiels – de type CNI.

Ma profession figure-t-elle dans les données piratées ?

Non. La fédération n'a pas ces informations dans ses bases de données.

Le service officiel qui en dispose est le SIA – le Système d'Information sur les Armes.

Je m'inquiète car mon adresse peut figurer dans les données susceptibles d'avoir été compromises. Que dois-je faire ? Dois-je porter plainte ?

D'abord, nous vous présentons toutes nos excuses pour l'inquiétude qu'une telle situation peut générer et les désagréments causés.

Nous vous appelons à la plus grande vigilance.

Nous leur rappelons les obligations légales liées au stockage d'une arme.

Les licenciés qui le souhaitent peuvent également :

- Signaler au service de police ou de gendarmerie dont ils dépendent l'incident ayant pu compromettre leurs données personnelles ;
 - Alerter dans ce signalement sur leurs craintes ou les risques connexes qu'ils redoutent en ce qui le concerne compte-tenu de la nature des données personnelles sensibles susceptibles d'avoir été compromises ;
 - Solliciter dans ce cadre la mise en place opérationnelle de mesures de protection préventives.
- Les autorités publiques ont également été informées de la situation.

Les systèmes d'information de la Fédération Française de Tir étaient-ils à jour et suffisamment protégés ?

Notre système était à jour et correctement maintenu.

Malheureusement, aucun système informatique n'est infaillible face à la cybercriminalité.

Nous avons identifié l'origine de l'incident rapidement et avons pris les mesures correctives qui s'imposaient dès cet instant.

En plus de ces mesures, nous travaillons actuellement à un renforcement de la sécurisation de nos systèmes d'information et avons également décidé de lancer un audit complet de notre infrastructure afin de renforcer notre capacité à lutter contre les cyber-attaques.

Avez-vous prévenu le ministère de l'Intérieur, les préfectures et les armureries ?

Nous avons prévenu l'ensemble des services de l'Etat qui doivent l'être et sommes en lien étroits avec eux.

Les préfectures et les armuriers sont informés de l'incident via le ministère de l'Intérieur qui les a lui-même appelés à la vigilance.

Comment savoir si les mails que je reçois de la part de certains services de l'Etat ou de tout autre émetteur faisant référence à ma licence n'est pas un mail frauduleux ?

Pour vous protéger, voici quelques conseils simples pour reconnaître un email frauduleux :

- Vérifiez l'expéditeur : Un email frauduleux vient souvent d'une adresse qui ressemble à celle d'une entreprise légitime, mais avec une faute, un domaine étrange, ou une adresse Gmail, Hotmail, etc., qui ne correspond pas à l'organisation.
- Méfiance face à l'urgence : Les emails frauduleux insistent souvent pour que vous agissiez rapidement, sous peine de conséquences graves. Ils jouent sur la peur ou l'urgence « Votre compte sera suspendu si vous ne répondez pas avant X ».
- Ne cliquez pas sur les liens suspects : Survolez les liens sans cliquer pour vérifier qu'ils correspondent bien à l'adresse officielle. Les liens dans les mails frauduleux mènent souvent vers des sites imitant des sites officiels, destinés à voler vos informations.
- Attention aux pièces jointes étranges : N'ouvrez pas les pièces jointes si vous ne les attendiez pas ou si elles ont une extension inhabituelle (.exe, .scr, .zip).
- Absence de personnalisation : Les emails frauduleux emploient souvent des formules génériques (« Cher client », « Utilisateur ») au lieu de votre nom.
- Recherchez les fautes : Les mails frauduleux contiennent souvent des erreurs d'orthographe, de grammaire ou de syntaxe.
- Méfiez-vous des demandes d'informations personnelles : Ne transmettez jamais vos mots de passe, numéros bancaires, ou autres données sensibles par email.

Si vous recevez un email suspect, ne répondez pas, ne cliquez sur aucun lien et ne téléchargez pas de pièces jointes. Il est recommandé de signaler ce mail à votre fournisseur de messagerie (via la fonction « Signaler comme spam » ou « Phishing ») et à l'entité usurpée si vous pouvez identifier son origine.

Comment expliquer le délai entre l'incident et la communication faite aux licenciés ?

Compte tenu de la nature de l'incident et de notre activité, nous étions tenus d'informer dans un premier temps les autorités compétentes – dont les services de l'Etat – et de nous assurer qu'elles avaient bien pris connaissance de la situation avant de communiquer plus largement.

Nous avons communiqué à l'ensemble des licenciés dès que nous avons été en mesure de le faire.

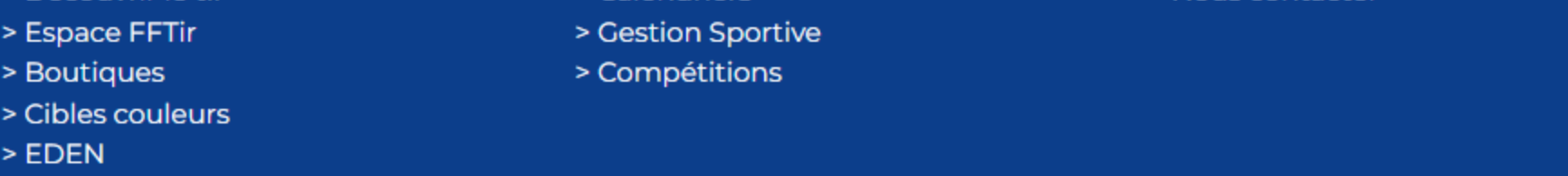
Pourquoi ne pouvez-vous pas me dire à titre individuel si mes données personnelles sont concernées ?

A ce stade, une enquête est toujours en cours afin de déterminer si les données concernées par l'incident ont été compromises ou non. Cela signifie que nous ne sommes pas encore capables de déterminer si les données concernées ni quelles données parmi elles auraient pu être exploitées illégalement.

Ce que nous savons, c'est que les données concernées pourraient potentiellement toucher l'ensemble des licenciés.

C'est la raison pour laquelle nous les informons tous sans pouvoir apporter de réponse individuelle.

Partager ce contenu



Plan du site

- > Fédération Française de Tir
- > Où pratiquer
- > Découvrir le tir
- > Espace FFTir
- > Boutiques
- > Cibles couleurs
- > EDEN

- > Actualités
- > C.N.T.S.
- > Calendriers
- > Gestion Sportive
- > Compétitions

- > Archives
- > Espace presse
- > Nous contacter

Informations légales

- > Politique de confidentialité
- > Politique de confidentialité des mineurs
- > Conditions générales d'utilisation

