

Renforcement de la vigilance face aux tentatives de fraude

Madame, Monsieur,

À la suite de l'acte de cybermalveillance ayant visé logiciel fédéral Gest'Hand, nous souhaitons vous rappeler les principales mesures de prévention à adopter afin de limiter les risques de fraude et d'hameçonnage.

Cet incident survient dans un contexte de multiplication des cyberattaques visant les organisations sportives et institutionnelles. À la suite de l'incident de décembre 2025, la FFHandball avait engagé un renforcement de ses dispositifs de cybersécurité, cet effort se poursuit et s'accélère.

Des personnes malveillantes pourraient tenter de se faire passer pour la FFHandball, votre club, votre comité, votre ligue ou un prestataire, notamment par email, SMS ou téléphone. Leur objectif peut être de récupérer vos identifiants, vos mots de passe, vos données personnelles ou vos coordonnées bancaires.

Les mesures mises en œuvre

Afin de renforcer la protection des comptes et des données, les mesures suivantes ont été prises :

- sécurisation renforcée de l'outil et des données.
- neutralisation des accès identifiés comme suspects.
- réinitialisation des mots de passe des comptes utilisateurs concernés.
- renforcement des contrôles d'accès et de sécurité.
- durcissement des règles relatives aux mots de passe.
- surveillance accrue des activités inhabituelles.
- amélioration continue des dispositifs de cybersécurité.
- signalement de l'incident aux autorités compétentes et dépôt d'une plainte.

Les bons réflexes à adopter

Nous vous invitons à rester particulièrement vigilants face à toute communication inhabituelle

- ne cliquez pas sur un lien reçu par email ou SMS si vous avez un doute sur son origine.
- ne communiquez jamais votre mot de passe, vos codes de validation, vos identifiants ou vos coordonnées bancaires par email, SMS ou téléphone.
- vérifiez attentivement l'adresse de l'expéditeur, le numéro de téléphone et le contenu du message.
- méfiez-vous des messages urgents, alarmants ou vous demandant une action immédiate.
- n'ouvrez pas les pièces jointes inattendues ou provenant d'un expéditeur inconnu.
- avant toute action, contactez directement votre club, votre comité, votre ligue ou la FFHandball en utilisant leurs coordonnées habituelles, et non celles indiquées dans le message reçu.
- utilisez un mot de passe unique et complexe pour chaque service.
- activez l'authentification à deux facteurs lorsqu'elle est disponible.
- signalez tout message suspect et supprimez-le sans y répondre.

Vous pouvez consulter les conseils officiels contre l'hameçonnage pour plus d'informations via le bouton ci-dessous :

Conseils officiels contre l'hameçonnage