MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Service Central des Armes et Explosifs

HYGIÈNE NUMÉRIQUE MAITRISÉE, SÉCURITÉ ASSURÉE

Un râtelier bien protégé physiquement doit l'être aussi numériquement. Le SIA comporte des informations sensibles relatives à vos armes. Suivre ces recommandations constitue la première ligne de défense contre les d'intrusion et la compromission des données.

1. Protégez vos comptes



Utilisez un mot de passe long et unique pour votre compte SIA.

Activez la double authentification à deux facteurs (2FA) dès que possible.

2. Ne partagez pas



Limitez les données et informations que vous partagez en ligne telles que votre adresse,
vos coordonnées, lieu de tir, photos des armes, vos équipements, vos habitudes...).

3. Evitez les Wifi publics



Evitez d'accéder à votre compte SIA depuis un Wi-Fi public ou un appareil partagé.

Utilisez un VPN si nécessaire.

4. Vigilance face aux vols par ruse

Méfiez-vous des faux professionnels
N'ouvrez pas à un inconnu, même en uniforme.
Demandez une carte professionnelle.
Gardez la porte verrouillée pendant toute la vérification.

Ne répondez pas aux mails et sms suspects.
Ne communiquez jamais vos informations personnelles et mot de passe surtout par téléphone.



En cas de doute, **appelez le 17** ou contactez directement la préfecture ou le SCAE.

Ne laissez jamais un visiteur seul dans votre domicile ou sans surveillance.

Ne révélez jamais l'emplacement de vos armes, objets de valeur, argent ou codes confidentiels.

5. Sécurisez vos appareils



Verrouillez vos appareils (PIN, mot de passe, empreinte, reconnaissance faciale) et chiffrez les données si possible. Mettez-les à jour régulièrement.

6. Sauvegardez vos données importantes



Conservez une sauvegarde chiffrée de vos documents importants (licences, factures, photos des armes) sur un support sécurisé (disque dur externe, cloud fiable).

7. Déconnectez-vous et fermez vos sessions



Pensez à vous déconnecter après chaque session, surtout sur les sites administratifs ou sensibles. Evitez d'enregistrer vos identifiants sur les navigateurs.

EN CAS DE PERTE, VOL OU ACCÈS SUSPECT :
Changez immédiatement vos mots de passe, contactez votre préfecture ou le support informatique SIA et déposez plainte si nécessaire.

Plus d'informations sur la sécurité numérique :
www.cybermalveillance.gouv.fr

POLICE NATIONALE

Gendarmerie nationale