Sécurité et protection des données à caractère personnel traitées dans les applicatifs gérés par le GIP SNE

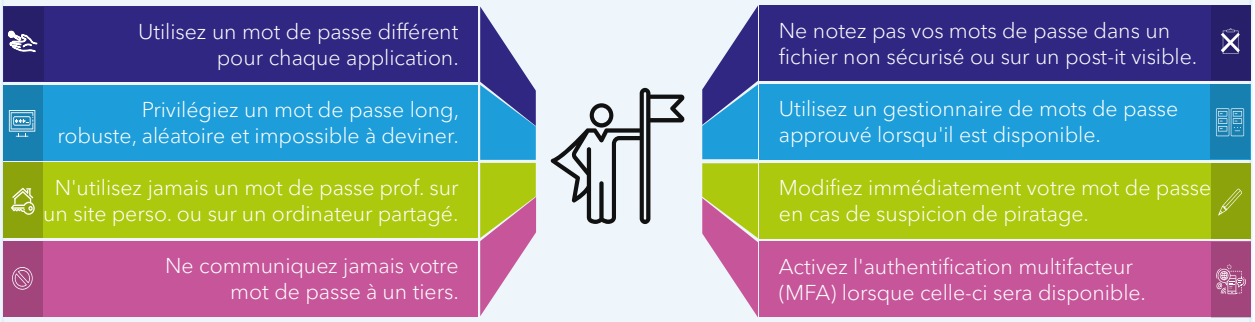
L'actualité récente des cyberattaques visant des administrations rappelle la vigilance collective nécessaire à avoir concernant l'accès aux données personnelles des demandeurs de logement social. Cette sécurité relève de la responsabilité de tous les professionnels habilités, que l'accès s'effectue directement via les applications du GIP SNE ou indirectement par interface avec un SI privatif ou une application tierce (SYPLO/COMDALO).

COMMENT JE SECURISE L'ACCES AUX OUTILS COMPORTANT DES DONNEES A CARACTERE PERSONNEL ?

L'accès aux données à caractère personnel par une personne non habilitée constitue une violation de données. L'accès illégitime peut intervenir à la suite d'une habilitation délivrée de manière indue ou de l'utilisation des identifiants d'un professionnel dûment habilité par une personne non habilitée.

Je peux agir en :

- Vérifiant si le professionnel demandant un accès aux applications est dûment habilité (cf. https://sne.info.application.logement.gouv.fr/description-du-sne/conditions-dacces-au-sne) et si l'adresse email du professionnel est bien nominative et comporte le nom de domaine de l'entité de rattachement.
- Signalant au gestionnaire territorial tout départ d'un professionnel habilité afin de supprimer ses accès.
- Respectant les règles suivantes de bonnes pratiques concernant la sécurisation de mes propres identifiants me permettant d'accéder aux applicatifs gérés par le GIP SNE :



Pour en apprendre plus sur la gestion de vos mots de passe, nous vous invitons à consulter la page : "Pourquoi et comment bien gérer ses mots de passe ?" sur cybermalveillance.gouv.fr.

COMMENT LUTTER CONTRE LES USURPATIONS D'IDENTITE ?

La technique du "phishing" ou "hameçonnage", consiste pour l'essentiel à vous mettre en confiance pour prendre la main sur vos données, et ainsi accéder à votre insu aux données des demandeurs. Ainsi, vous pouvez être vous-même victime d'une tentative d'usurpation d'identité ou être le vecteur par lequel le hackeur va pouvoir accéder aux données personnelles de demandeurs qui pourraient alors être victimes d'usurpation d'identité.

L'usurpation d'identité peut engendrer de graves conséquences pour les personnes concernées (interdictions bancaires, amendes, etc).

Je peux agir en étant particulièrement vigilant à la suite de la réception d'emails et SMS/appels suspects et en appliquant les recommandations suivantes :

JE VERIFIE L'ADRESSE DE L'EXPEDITEUR
Un passage de la souris sur l'adresse de l'expéditeur permet de contrôler l'adresse email de l'expéditeur.

JE ME MEFIE DES URGENCES
Les pirates créent un sentiment d'urgence auprès de leurs victimes. Un ton alarmiste ou des demandes inhabituelles doivent susciter votre vigilance.

JE NE CLIQUE PAS TOUT DE SUITE SUR LES LIENS
Passez d'abord votre souris sur les liens pour vérifier l'URL avant de cliquer. En cas de doute, prenez contact avec l'expéditeur par un autre canal tel le téléphone.

JE N'OUVRE PAS LES PIECES JOINTES DOUTEUSES
Si vous n'êtes pas sûr de l'expéditeur et/ou du contenu du message, n'ouvrez pas la pièce jointe. Si vous êtes sensé connaître l'expéditeur, demandez-lui confirmation qu'il vous l'a bien envoyée.

JE NE TRANSMETS JAMAIS MES DONNEES DE CONNEXION
Vos identifiants et mots de passe ne doivent jamais être transmis par email.

LES INTERDITS ET LES BONS REFLEXES :

❌ Ne pas adresser de données à caractère personnel (fichiers de demandeurs, liste de contacts, pièces justificatives, etc.) par simple email sans avoir sécurisé l'accès au fichier et privilégier le dépôt des fichiers sur des serveurs sécurisés.

❌ Ne jamais transférer de données à caractère personnel à un tiers non habilité ou dans une IA générative (Claude AI, ChatGPT, Copilote, etc.)

☑ Limiter les exports de données à caractère personnel et minimiser le périmètre des données au strict nécessaire (toujours questionner la finalité, la légalité et la sécurité des données).

☑ Limiter la sauvegarde de fichiers Excel et CSV comportant des données à caractère personnel le temps nécessaire au traitement, puis supprimer les fichiers concernés.